

10/804,097

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 4 年    3 月    1 日  
Date of Application:

願 番 号                      特 願 2 0 0 4 - 0 5 6 7 6 4  
Application Number:  
[ J P 2 0 0 4 - 0 5 6 7 6 4 ]

願 人                      株 式 会 社 リ コ ー  
Applicant(s):

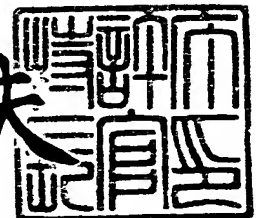
CERTIFIED COPY OF  
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2 0 0 4 年    4 月 1 2 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 4 - 3 0 2 9 7 7 5

【書類名】 特許願  
【整理番号】 0401295  
【提出日】 平成16年 3月 1日  
【あて先】 特許庁長官 殿  
【国際特許分類】 H04L 9/14  
【発明者】  
    【住所又は居所】 東京都大田区中馬込 1丁目 3番 6号 株式会社リコー内  
    【氏名】 榎田 寛朗  
【特許出願人】  
    【識別番号】 000006747  
    【住所又は居所】 東京都大田区中馬込 1丁目 3番 6号  
    【氏名又は名称】 株式会社リコー  
    【代表者】 桜井 正光  
【代理人】  
    【識別番号】 100080931  
    【住所又は居所】 東京都豊島区東池袋 1丁目 20番 2号 池袋ホワイトハウスビル  
    818号  
    【弁理士】  
    【氏名又は名称】 大澤 敬  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2003- 75278  
    【出願日】 平成15年 3月19日  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2003- 96129  
    【出願日】 平成15年 3月31日  
【手数料の表示】  
    【予納台帳番号】 014498  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9809113

**【書類名】 特許請求の範囲****【請求項 1】**

クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、

前記デジタル証明書管理装置に、

前記サーバが前記認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、

前記新証明鍵を前記クライアントに送信する第 1 の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第 2 の送信手段とを設け、

該第 2 の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。

**【請求項 2】**

請求項 1 記載のデジタル証明書管理システムであって、

前記デジタル証明書管理装置の前記証明鍵更新手段に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段を設け、

前記第 1 の送信手段は、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信する手段であり、

前記クライアントに、

前記デジタル証明書管理装置から前記証明鍵証明書に含まれる証明鍵を受信した場合に、受信した証明鍵証明書の正当性を従前の証明鍵を用いて確認し、そこに含まれる証明鍵が適当なものであると判断した場合に該証明鍵を記憶する手段を設けたことを特徴とするデジタル証明書管理システム。

**【請求項 3】**

請求項 1 記載のデジタル証明書管理システムであって、

前記デジタル証明書管理装置の前記証明鍵更新手段に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 1 の証明鍵証明書を取得する手段と、

前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 2 の証明鍵証明書を取得する手段とを設け、

前記第 1 の送信手段は、前記新証明鍵を前記第 1 及び第 2 の証明鍵証明書の形式でそれぞれ前記クライアントに送信する手段であり、

前記クライアントに、

前記デジタル証明書管理装置から前記第 1 の証明鍵証明書を受信した場合に、該証明書の正当性を従前の証明鍵を用いて確認し、これが適当なものであると判断した場合に該証明書を記憶する手段と、

前記デジタル証明書管理装置から前記第 2 の証明鍵証明書を受信した場合に、該証明書の正当性を前記第 1 の証明鍵証明書に含まれる前記新証明鍵を用いて確認し、前記第 2 の証明鍵証明書が適当なものであると判断した場合に、該証明書を記憶すると共に従前の証明鍵証明書及び前記第 1 の証明鍵証明書を削除する手段とを設け、

前記デジタル証明書管理装置の前記第 1 の送信手段は、前記第 2 の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信し

た旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。

【請求項 4】

クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、

前記デジタル証明書管理装置に、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第 1 の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第 2 の送信手段とを設け、

該第 2 の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であり、

前記第 1 の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。

【請求項 5】

請求項 4 記載の証明書管理システムであって、

前記第 1 の送信手段を、前記新証明鍵を、前記新クライアント証明書と同時あるいはそれより前に前記クライアントに送信する手段とし、

前記第 2 の送信手段を、前記新証明鍵を、前記新サーバ証明書と同時あるいはそれより前に前記サーバに送信する手段としたことを特徴とする証明書管理システム。

【請求項 6】

クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、

前記デジタル証明書管理装置に、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第 1 の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第 2 の送信手段とを設け、

前記第 1 の送信手段が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する手段であり、

前記第 2 の送信手段が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する手段であることを特徴とするデジタル証明書管理システム。



**【請求項7】**

前記サーバに、前記デジタル証明書管理装置と前記クライアントとの間の通信を仲介する手段を設け、

前記デジタル証明書管理装置と前記クライアントとは前記サーバを介して通信を行い、該サーバが、前記デジタル証明書管理装置の第1の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するようにしたことを特徴とする請求項1乃至6のいずれか一項記載のデジタル証明書管理システム。

**【請求項8】**

前記クライアントに、前記デジタル証明書管理装置と前記サーバとの間の通信を仲介する手段を設け、

前記デジタル証明書管理装置と前記サーバとは前記クライアントを介して通信を行い、該クライアントが、前記デジタル証明書管理装置の第2の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するようにしたことを特徴とする請求項1乃至6のいずれか一項記載のデジタル証明書管理システム。

**【請求項9】**

請求項1乃至8のいずれか一項記載のデジタル証明書管理システムであって、

前記クライアントと前記サーバが行う認証は、SSL又はTLSのプロトコルに従った認証であり、

前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理システム。

**【請求項10】**

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、

前記クライアントと前記サーバとの間で通信を確立する際の認証に前記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、

前記新証明鍵を前記クライアントに送信する第1の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第2の送信手段とを設け、

該第2の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理装置。

**【請求項11】**

請求項10記載のデジタル証明書管理装置であって、

前記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段を設け、

前記第1の送信手段が、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信してここに含まれる証明鍵を記憶するよう要求する手段であることを特徴とするデジタル証明書管理装置。

**【請求項12】**

請求項10記載のデジタル証明書管理装置であって、

前記証明鍵更新手段に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む

第1の証明鍵証明書を取得する手段と、

前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第2の証明鍵証明書を取得する手段とを設け、

前記第1の送信手段が、前記新証明鍵を前記第1及び第2の証明鍵証明書の形式でそれぞれ前記クライアントに送信する手段であって、前記クライアントに、前記第2の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び前記第1の証明鍵証明書を削除させる手段を有し、前記第2の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に行うようにしたことを特徴とするデジタル証明書管理装置。

【請求項13】

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、

前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第1の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第2の送信手段とを設け、

該第2の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であり、

前記第1の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理装置。

【請求項14】

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、

前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第1の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第2の送信手段とを設け、

前記第1の送信手段が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する手段であり、

前記第2の送信手段が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する手段であることを特徴とするデジタル証明書管理装置。

【請求項15】

前記クライアントとは前記サーバを介して通信を行い、

該サーバは、前記第1の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書をを用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するサーバで

あることを特徴とする請求項 10 乃至 14 のいずれか一項記載のデジタル証明書管理装置。

【請求項 16】

前記サーバとは前記クライアントを介して通信を行い、

該クライアントは、前記第 2 の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するクライアントであることを特徴とする請求項 10 乃至 14 のいずれか一項記載のデジタル証明書管理装置。

【請求項 17】

請求項 10 乃至 16 のいずれか一項記載のデジタル証明書管理装置であって、

前記認証は、SSL又はTLSのプロトコルに従った認証であり、

前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理装置。

【請求項 18】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記サーバが前記認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、前記新証明鍵を前記クライアントに送信する第 1 の手順を実行し、該クライアントから該新証明鍵を受信した旨の情報を受信した後で、前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第 2 の手順を実行することを特徴とするデジタル証明書管理方法。

【請求項 19】

請求項 18 記載のデジタル証明書管理方法であって、

前記証明鍵の更新の際に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手順をさらに実行し、

前記第 1 の手順は、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信する手順であり、

前記クライアントに前記証明鍵証明書を送信する場合に、該証明鍵証明書の正当性を記憶している従前の証明鍵を用いて確認させ、そこに含まれる証明鍵が適当なものであると判断した場合に該証明鍵を記憶させることを特徴とするデジタル証明書管理方法。

【請求項 20】

請求項 18 記載のデジタル証明書管理方法であって、

前記証明鍵の更新の際に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 1 の証明鍵証明書を取得する手順と、

前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 2 の証明鍵証明書を取得する手順とをさらに実行し、

前記第 1 の手順において、前記新証明鍵を前記第 1 の証明鍵証明書の形式で前記クライアントに送信し、

前記第 2 の手順の完了後、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に、前記第 2 の証明鍵証明書を前記クライアントに送信する手順を実行し、

前記クライアントに前記第1の証明鍵証明書を送信する際に、該証明書の正当性を従前の証明鍵を用いて確認させ、これが適当なものであると判断した場合に該証明書を記憶させ、

前記クライアントに前記第2の証明鍵証明書を送信する際に、該証明書の正当性を前記第1の証明鍵証明書に含まれる前記新証明鍵を用いて確認させ、前記第2の証明鍵証明書が適当なものであると判断した場合に、該証明書を記憶させると共に従前の証明鍵証明書及び前記第1の証明鍵証明書を削除させることを特徴とするデジタル証明書管理方法。

【請求項 21】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、

前記新証明鍵を前記サーバに送信する第1の手順と、

前記新証明鍵を前記クライアントに送信する第2の手順と、

前記クライアントのための新デジタル証明書である新クライアント証明書を前記クライアントに送信する第3の手順と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第4の手順とを適当な順番で実行し、

このとき少なくとも、前記第4の手順を、前記第2の手順の完了後、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に、前記第3の手順を、前記第1の手順の完了後、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に実行するようにしたことを特徴とするデジタル証明書管理方法。

【請求項 22】

請求項 21 記載のデジタル証明書管理方法であって、

前記第3の手順を前記第2の手順と同時に又はその完了後に、前記第4の手順を前記第1の手順と同時に又はその完了後に実行するようにしたことを特徴とするデジタル証明書管理方法。

【請求項 23】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、

前記新証明鍵を前記サーバに送信する第1の手順と、

前記新証明鍵を前記クライアントに送信する第2の手順と、

前記クライアントのための新デジタル証明書である新クライアント証明書を前記クライアントに送信する第3の手順と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第4の手順とを適当な順番で実行し、

このとき、前記第2の手順と前記第3の手順とを一括して実行し、これらの手順の完了後、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記第1の手順と前記第4の手順とを一括して実行するようにしたことを特徴とするデジタル証明書管理方法。

【請求項24】

前記デジタル証明書管理装置と前記クライアントとは前記サーバを介して通信を行い、該サーバが、前記デジタル証明書管理装置が前記第2及び／又は第3の手順で前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するようにしたことを特徴とする請求項18乃至23のいずれか一項記載のデジタル証明書管理方法。

【請求項25】

前記デジタル証明書管理装置と前記サーバとは前記クライアントを介して通信を行い、該クライアントが、前記デジタル証明書管理装置が前記第1及び／又は第4の手順で前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するようにしたことを特徴とする請求項18乃至23のいずれか一項記載のデジタル証明書管理方法。

【請求項26】

請求項18乃至25のいずれか一項記載のデジタル証明書管理方法であって、前記クライアントと前記サーバとの間の前記認証は、SSL又はTLSのプロトコルに従った認証であり、前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理方法。

【請求項27】

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、前記クライアントと前記サーバとの間で通信を確立する際の認証に前記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、前記コンピュータを、更新用の新証明鍵を取得する手段と、該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、前記新証明鍵を前記クライアントに送信する第1の送信手段と、前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第2の送信手段として機能させるためのプログラムを含み、該第2の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行うようにしたことを特徴とするプログラム。

【請求項28】

請求項27記載のプログラムであって、前記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含み、前記第1の送信手段が、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信するようにしたことを特徴とするプログラム。

【請求項29】

請求項 27 記載のプログラムであって、  
前記コンピュータを、  
従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 1 の証明鍵証明書を取得する手段と、  
前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第 2 の証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含み、  
前記第 1 の送信手段が、前記新証明鍵を前記第 1 及び第 2 の証明鍵証明書の形式でそれぞれ前記クライアントに送信し、前記クライアントに、前記第 2 の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び前記第 1 の証明鍵証明書を削除させる機能を有し、さらに、前記第 2 の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に行う機能を有することを特徴とするプログラム。

【請求項 30】

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、  
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、  
前記コンピュータを、  
更新用の新証明鍵を取得する手段と、  
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、  
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第 1 の送信手段と、  
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第 2 の送信手段として機能させるためのプログラムを含み、  
該第 2 の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行うようにし、  
前記第 1 の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行うようにしたことを特徴とするプログラム。

【請求項 31】

クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、  
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、  
前記コンピュータを、  
更新用の新証明鍵を取得する手段と、  
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、  
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第 1 の送信手段と、  
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第 2 の送信手段として機能させるためのプログラムを含み、  
前記第 1 の送信手段の機能が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する機能であり、  
前記第 2 の送信手段の機能が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する機能であることを特徴とするプログラム。

**【請求項 3 2】**

前記コンピュータを、前記クライアントとは前記サーバを介して通信を行うよう機能させるためのプログラムを含み、

該サーバは、前記第 1 の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するサーバであることを特徴とする請求項 2 7 乃至 3 1 のいずれか一項記載のプログラム。

**【請求項 3 3】**

前記コンピュータを、前記サーバとは前記クライアントを介して通信を行うよう機能させるためのプログラムを含み、

該クライアントは、前記第 2 の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するクライアントであることを特徴とする請求項 2 7 乃至 3 1 のいずれか一項記載のプログラム。

**【請求項 3 4】**

請求項 2 7 乃至 3 3 のいずれか一項記載のプログラムであって、

前記認証は、SSL 又は TLS のプロトコルに従った認証であり、

前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするプログラム。

**【書類名】明細書**

**【発明の名称】** デジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法およびプログラム

**【技術分野】**

**【0001】**。

この発明は、デジタル証明書管理装置によってクライアント・サーバシステムを構成するクライアントとサーバの間の認証処理に用いるデジタル証明書を管理するデジタル証明書管理システム、このようなシステムを構成するデジタル証明書管理装置、このようにデジタル証明書を管理するデジタル証明書管理方法、およびコンピュータを上記のデジタル証明書管理装置として機能させるためのプログラムに関する。

**【背景技術】**

**【0002】**

従来から、PC等のコンピュータを複数台ネットワークを介して通信可能に接続し、少なくとも1台をサーバ装置（サーバ）、別の少なくとも1台をクライアント装置（クライアント）としたクライアント・サーバシステムを構成することが行われている。

このようなクライアント・サーバシステムにおいては、クライアント装置からサーバ装置に要求を送信し、サーバ装置がその要求に従った処理を行ってクライアント装置に対して応答を返す。そして、このようなクライアント・サーバシステムは、クライアント装置から商品の注文要求を送信し、サーバ装置においてその注文を受け付けるといった、いわゆる電子商取引にも広く用いられるようになってきている。また、種々の電子装置にクライアント装置あるいはサーバ装置の機能を持たせてネットワークを介して接続し、相互間の通信によって電子装置の遠隔管理を行うシステムも提案されている。

**【0003】**

このような場合においては、通信相手が適切か、あるいは送信される情報が改竄されていないかといった確認が重要である。また、特にインターネットにおいては、情報が通信相手に到達するまでに無関係なコンピュータを経由する機会が多いことから、機密情報を送信する場合、その内容を盗み見られないようにする必要もある。そして、このような要求に応える通信プロトコルとして、例えばSSL（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、情報の暗号化により改竄及び盗聴の防止を図ることができる。

**【0004】**

ここで、公開鍵暗号方式を用いて認証処理を行う場合の通信手順及びその際に使用するデジタル証明書について説明する。なおここでは、クライアント装置がサーバ装置を認証する場合を例として説明する。

この場合、認証処理を行うために、サーバ装置側にサーバ私有鍵及びサーバ公開鍵証明書（サーバ証明書）を記憶させると共に、クライアント装置側にルート鍵証明書を記憶させておく。ここで、サーバ私有鍵は、認証局（CA：certificate authority）がサーバ装置に対して発行した私有鍵である。そして、サーバ公開鍵証明書は、その私有鍵と対応する公開鍵にCAがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、CAがデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。

**【0005】**

図41にこれらの関係を示す。

図41（a）に示すように、サーバ公開鍵は、サーバ私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（CA）、発行相手（サーバ装置）、有効期限等の情報を含む書誌情報とによって構成される。そして、CAは、鍵本体や書誌情報が改竄されていないことを示すため、サーバ公開鍵をハッシュ処理して得たハッシュ値を、ルート私有鍵を用いて暗号化し、デジタル署名としてサーバ公開鍵に付す。またこ



の際に、デジタル署名に用いるルート私有鍵の識別情報を署名鍵情報として公開鍵の書誌情報に加える。そして、このデジタル署名を付した公開鍵証明書が、サーバ公開鍵証明書である。

#### 【0006】

このサーバ公開鍵証明書を認証処理に用いる場合には、ここに含まれるデジタル署名を、ルート私有鍵と対応する公開鍵であるルート鍵の鍵本体を用いて復号化する。この復号化が正常に行われれば、デジタル署名が確かにCAによって付されたことがわかる。また、サーバ公開鍵部分をハッシュ処理して得たハッシュ値と、復号して得たハッシュ値とが一致すれば、鍵自体も損傷や改竄を受けていないことがわかる。さらに、受信したデータをこのサーバ公開鍵を用いて正常に復号化できれば、そのデータは、サーバ私有鍵の持ち主、つまりサーバ装置から送信されたものであることがわかる。あとは、書誌情報を参照して、CAの信頼性やサーバ装置の登録有無等によって認証の正否を決定すればよい。

#### 【0007】

ここで、認証を行うためには、ルート鍵を予め記憶しておく必要があるが、このルート鍵も、図41(b)に示すように、CAがデジタル署名を付したルート鍵証明書として記憶しておく。このルート鍵証明書は、自身に含まれる公開鍵でデジタル署名を復号化可能な、自己署名形式である。そして、ルート鍵を使用する際に、そのルート鍵証明書に含まれる鍵本体を用いてデジタル署名を復号化し、ルート鍵をハッシュ処理して得たハッシュ値と比較する。これが一致すれば、ルート鍵が破損等していないことを確認できるのである。

#### 【0008】

そして、以上のようなクライアント装置とサーバ装置とによって構成されるクライアント・サーバシステムにおいてクライアント装置がサーバ装置に通信を要求する場合、これらの各装置はそれぞれ以下のような処理を行う。

まずサーバ装置は、クライアント装置からの通信要求に応じて乱数を生成すると共に、これをサーバ私有鍵で暗号化し、その暗号化した乱数をサーバ公開鍵証明書と共にクライアント装置に送信する。

すると、これを受信したクライアント装置は、受信したサーバ公開鍵証明書の正当性をルート鍵証明書を用いて確認する。これには、上述のように損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置が適当な通信相手であることを確認する処理を含む。

#### 【0009】

そして確認ができると、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて受信した乱数を復号化する。ここで復号化が成功すれば、第1の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置から受信したものと確認できる。従って、以上の処理により、サーバ装置を正当な通信相手として認証することができる。

また、上記の公開鍵や私有鍵で暗号化して共通鍵暗号の鍵を交換するようにすれば、安全に共通鍵を交換し、通信内容を共通鍵暗号によって暗号化した安全な通信経路を確立することができる。

#### 【0010】

ところで、公開鍵暗号方式においては、鍵長にもよるが、時間をかければ公開鍵から私有鍵を導くことができる。そして、私有鍵がわかってしまえば、第3者がその私有鍵の持ち主になりすますことが可能になるので、認証の確実性や通信の安全性が保たれない。そこで、上述のように鍵に有効期限を設け、所定期間毎に鍵のセットを更新するというセキュリティポリシーを採用するユーザが増えている。このため、例えば上記のような認証処理を利用した遠隔管理システム等を提供する場合には、顧客に対し、鍵の更新が可能なシステムであるという保証を行う必要が生じている。これは、ルート鍵とルート私有鍵についても同様である。なお、鍵の更新事由としては、所定の有効期限の到来の他にも、私有鍵の第3者への漏洩が判明した場合等が考えられる。

このような鍵の更新に関する技術としては、例えば特許文献1に記載のものが挙げられ

る。

【特許文献1】特開平11-122238号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

しかしながら、特許文献1には、各装置に対して発行した鍵の更新に関する記載はあるが、ルート鍵の更新についての記載はない。

公開鍵暗号方式の場合、各装置に発行した鍵のペアを更新する場合には、その装置には新たな私有鍵に対応した新たな公開鍵証明書が記憶されることになり、通信相手にこれを渡せば、上述のような認証処理を支障なく行うことができる。

しかし、ルート鍵を更新する場合、新たなルート鍵では従前のデジタル証明書に付されたデジタル署名を復号化することができないため、新たなルート鍵と対応する新たなルート私有鍵を用いて各装置の公開鍵証明書を作成し直し、これを配布しなければ、認証処理の実行に支障を来してしまう（ただし、各装置の私有鍵は必ずしも更新する必要はない）。

【0012】

そして、認証処理に支障を来さずにこのようなルート鍵を更新する方式が知られていなかったため、更新の必要な装置にルート鍵をネットワークを介して安全に送信することができなかった。そこで、ルート鍵証明書や新たな公開鍵証明書を別の安全な経路で各装置に届ける必要があった。すなわち、ルート鍵更新用の特別な通信経路を設ける必要があったのである。

この経路としては、例えば書留郵便が考えられ、証明書のデータを記録したメモ리카ードやフレキシブルディスク等の記録媒体を装置の管理者に書留郵便で送付し、管理者が装置の鍵を更新するという方式が考えられる。しかし、この方式では、クライアントやサーバの各装置について十分な知識を持った管理者がいる場合にしか適用できないし、CA側は記録媒体を送付した後の処理については装置の管理者を信用するしかなかった。従って、管理者が更新処理を怠ったり誤ったりした場合には、認証処理が行えなくなってしまうという問題があった。

【0013】

一方管理者側も、受け取った証明書が正しいものであるか否かは、封筒やデータに記載された送り主の名称等を信用して判断するしかなく、CAの名を騙る別人から受け取ったニセの証明書を装置に記憶させてしまうといった危険は常につきまとうことになる。

また、CAやクライアント・サーバシステムによるサービスの提供者が、各装置の配置先にサービスマンを派遣して鍵の更新を行うことも考えられるが、広い地域でこのような方式を採用するには多数のサービス拠点が必要になり、コストが嵩むことになる。また、サービスマンの教育や不正防止、更新作業用の管理者IDの管理も問題となる。例えば、認証情報を手入力する単純な方式を採ろうとすると、退職したサービスマンについての更新権限を抹消するためには、各装置に記憶させている認証情報を変更する必要があるが、顧客先に設置された多数の装置にこのような変更を行うことは困難である。

【0014】

結局のところ、ネットワークを介さずに証明書の安全な配布経路を確保するためには、人間を信用する他なく、そこには欺瞞が入りこむ余地が出てしまう。そして、この余地を小さくするよう管理することはできるが、そのためには膨大なコストが生じてしまい、欺瞞の危険を考慮しなくて済むレベルの経路を証明書の配布のために構築することは、現実的ではなかった。

【0015】

また、更新用の特別な通信経路としては、通常の通信に使用するデジタル証明書及びルート鍵証明書とは別の、更新処理用デジタル証明書及び更新処理用ルート鍵証明書を用いた通信経路を用意することも考えられる。しかしながら、クライアント装置がサーバ装置を認証するシステムの場合、このような手法には問題がある。

すなわち、この場合サーバ装置は、クライアント装置から接続要求があった場合にデジタル証明書をクライアント装置に送信するのであるが、不特定多数のクライアント装置から任意のタイミングで接続要求を受け得るサーバ装置の場合、通常通信用と更新処理用のいずれのデジタル証明書をクライアント装置に送信すればよいかを適切に判断することは困難である。

#### 【0016】

仮に判断しようとするれば、例えば通信要求の際のソースエンドポイントアイデンティファイア、デスティネーションエンドポイントアイデンティファイアやURL (Uniform Resource Locator) のようなセッション識別子を利用して判断することが考えられる。しかしながら、このような判断を行うためには、クライアント装置側に通常通信か更新用通信かに応じてセッション識別子（例えばURL）を切替える機能を設けたり、サーバ装置側にソースエンドポイントアイデンティファイアと送信すべきデジタル証明書との対応関係を管理する機能を設けたりする必要が生じる。そして、このような機能を設けることは、コストアップにつながる。

#### 【0017】

従って、サーバ装置に、セッション識別子のような通信開始前の情報に基づいてクライアント装置に送信すべきデジタル証明書を選択する機能を設けることは避けたいという要求があった。また、同じプロトコルを利用して2種の通信経路を設けると、認証が失敗した場合に、それがデジタル証明書の異常によるものか、セッション識別子の誤りによるものかを区別し難いという問題も生じる。

以上のように、ルート鍵更新用の特別な通信経路を設けることは、コストや管理の負担を増すことになるので、このような特別な通信経路を設けることなく、ルート鍵を安全に更新したいという要求があった。

#### 【0018】

この発明は、このような問題を解決し、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることを目的とする。

#### 【課題を解決するための手段】

#### 【0019】

上記の目的を達成するため、この発明のデジタル証明書管理システムは、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記サーバが上記認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第2の送信手段とを設け、その第2の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたものである。

#### 【0020】

このようなデジタル証明書管理システムにおいて、上記デジタル証明書管理装置の上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段を設け、上記第1の送信手段を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信する手段とし、上記クライアントに、上記デジタル証明書管理装置から上記証明鍵証明書に含まれる証明鍵を受信した場合に、受信した証明鍵証明書の正当性を従前の証明鍵を用いて確認し、そこに含まれる証明鍵が適当なものであると判断した場合にその証明鍵を記憶する手段を設けるとよい。

#### 【0021】

あるいは、上記デジタル証明書管理装置の上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第1の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第2の証明鍵証明書を取得する手段とを設け、上記第1の送信手段を、上記新証明鍵を上記第1及び第2の証明鍵証明書の形式でそれぞれ上記クライアントに送信する手段とし、上記クライアントに、上記デジタル証明書管理装置から上記第1の証明鍵証明書を受信した場合に、その証明書の正当性を従前の証明鍵を用いて確認し、これが適当なものであると判断した場合にその証明書を記憶する手段と、上記デジタル証明書管理装置から上記第2の証明鍵証明書を受信した場合に、その証明書の正当性を上記第1の証明鍵証明書に含まれる上記新証明鍵を用いて確認し、上記第2の証明鍵証明書が適当なものであると判断した場合に、その証明書を記憶すると共に従前の証明鍵証明書及び上記第1の証明鍵証明書を削除する手段とを設け、上記デジタル証明書管理装置の上記第1の送信手段を、上記第2の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行う手段としてもよい。

#### 【0022】

また、この発明は、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段とを設け、その第2の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とし、上記第1の送信手段を、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたデジタル証明書管理システムも提供する。

このような証明書管理システムにおいて、上記第1の送信手段を、上記新証明鍵を、上記新クライアント証明書と同時あるいはそれより前に上記クライアントに送信する手段とし、上記第2の送信手段を、上記新証明鍵を、上記新サーバ証明書と同時あるいはそれより前に上記サーバに送信する手段とするとよい。

#### 【0023】

また、この発明は、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段とを設け、上記第1の送信手段を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する手段とし、上記第2の送信手段を、上記クライアントから上記新証明鍵を

受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する手段としたデジタル証明書管理システムも提供する。

【0024】

上記の各デジタル証明書管理システムにおいて、上記サーバに、上記デジタル証明書管理装置と上記クライアントとの間の通信を仲介する手段を設け、上記デジタル証明書管理装置と上記クライアントとは上記サーバを介して通信を行い、そのサーバが、上記デジタル証明書管理装置の第1の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するようにするとよい。

あるいは、上記クライアントに、上記デジタル証明書管理装置と上記サーバとの間の通信を仲介する手段を設け、上記デジタル証明書管理装置と上記サーバとは上記クライアントを介して通信を行い、そのクライアントが、上記デジタル証明書管理装置の第2の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するようにしてもよい。

さらに、上記クライアントと上記サーバが行う認証を、SSL又はTLSのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

【0025】

また、この発明のデジタル証明書管理装置は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第2の送信手段とを設け、その第2の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とするとよい。

【0026】

このようなデジタル証明書管理装置において、上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段を設け、上記第1の送信手段を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信してここに含まれる証明鍵を記憶するよう要求する手段とするとよい。

【0027】

あるいは、上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第1の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第2の証明鍵証明書を取得する手段とを設け、上記第1の送信手段を、上記新証明鍵を上記第1及び第2の証明鍵証明書の形式でそれぞれ上記クライアントに送信する手段とし、上記クライアントに、上記第2の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び上記第1の証明鍵証明書を削除させる手段を設け、上記第2の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行うようにするとよい。

【0028】

また、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に上記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明

鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段とを設け、その第2の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とし、上記第1の送信手段を、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたデジタル証明書管理装置も提供する。

#### 【0029】

さらにまた、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段とを設け、上記第1の送信手段を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する手段とし、上記第2の送信手段が、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する手段としたデジタル証明書管理装置も提供する。

#### 【0030】

また、これらのデジタル証明書管理装置において、上記クライアントとは上記サーバを介して通信を行うようにし、そのサーバを、上記第1の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するサーバとするとよい。

あるいは、上記サーバとは上記クライアントを介して通信を行うようにし、そのクライアントを、上記第2の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するクライアントとするとよい。

また、上記の各デジタル証明書管理装置において、上記認証を、SSL又はTLSのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

#### 【0031】

また、この発明のデジタル証明書管理方法は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記サーバが上記認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記クライアントに送信する第1の手順を実行した後、そのクライアントからその新証明鍵を受信した旨の情報を受信した後で、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第2の手順を実行するようにしたものである。

#### 【0032】



このようなデジタル証明書管理方法において、上記証明鍵の更新の際に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手順をさらに実行し、上記第1の手順を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信する手順とし、上記クライアントに上記証明鍵証明書を送信する場合に、その証明鍵証明書の正当性を記憶している従前の証明鍵を用いて確認させ、そこに含まれる証明鍵が適当なものであると判断した場合にその証明鍵を記憶させるようにするとよい。

#### 【0033】

あるいは、上記証明鍵の更新の際に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第1の証明鍵証明書を取得する手順と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第2の証明鍵証明書を取得する手順とをさらに実行し、上記第1の手順において、上記新証明鍵を上記第1の証明鍵証明書の形式で上記クライアントに送信し、上記第2の手順の完了後、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に、上記第2の証明鍵証明書を上記クライアントに送信する手順を実行し、上記クライアントに上記第1の証明鍵証明書を送信する際に、その証明書の正当性を従前の証明鍵を用いて確認させ、これが適当なものであると判断した場合にその証明書を記憶させ、上記クライアントに上記第2の証明鍵証明書を送信する際に、その証明書の正当性を上記第1の証明鍵証明書に含まれる上記新証明鍵を用いて確認させ、上記第2の証明鍵証明書が適当なものであると判断した場合に、その証明書を記憶させると共に従前の証明鍵証明書及び上記第1の証明鍵証明書を削除させるようにするとよい。

#### 【0034】

また、この発明は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記サーバに送信する第1の手順と、上記新証明鍵を上記クライアントに送信する第2の手順と、上記クライアントのための新デジタル証明書である新クライアント証明書を上記クライアントに送信する第3の手順と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第4の手順とを適当な順番で実行し、このとき少なくとも、上記第4の手順を、上記第2の手順の完了後、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に、上記第3の手順を、上記第1の手順の完了後、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に実行するようにしたデジタル証明書管理方法も提供する。

このようなデジタル証明書管理方法において、上記第3の手順を上記第2の手順と同時に又はその完了後に、上記第4の手順を上記第1の手順と同時に又はその完了後に実行するようにするとよい。

#### 【0035】

また、この発明は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記サーバに送信する第1の手順と、上記新証明鍵を上記クライアントに送信する第2の手順と、上記クライアントのための新デジタル証明書である新クラ

クライアント証明書を上記クライアントに送信する第3の手順と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第4の手順とを適当な順番で実行し、このとき、上記第2の手順と上記第3の手順とを一括して実行し、これらの手順の完了後、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記第1の手順と上記第4の手順とを一括して実行するようにしたデジタル証明書管理方法も提供する。

#### 【0036】

また、上記の各デジタル証明書管理方法において、上記デジタル証明書管理装置と上記クライアントとが上記サーバを介して通信を行い、そのサーバが、上記デジタル証明書管理装置が上記第2及び／又は第3の手順で上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するようにするとよい。

あるいは、上記デジタル証明書管理装置と上記サーバとが上記クライアントを介して通信を行い、そのクライアントが、上記デジタル証明書管理装置が上記第1及び／又は第4の手順で上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するようにするとよい。

さらに、以上の各デジタル証明書管理方法において、上記クライアントと上記サーバとの間の上記認証を、SSL又はTLSのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

#### 【0037】

また、この発明のプログラムは、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の認証に上記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第2の送信手段として機能させるためのプログラムを含め、その第2の送信手段が、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行うようにしたものである。

#### 【0038】

このようなプログラムにおいて、上記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含め、上記第1の送信手段が、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信するようにするとよい。

#### 【0039】

あるいは、上記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第1の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第2の証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含め、上記第1の送信手段に、上記新証明鍵を上記第1及び第2の証明鍵証明書の形式でそれぞれ上記クライアントに送信し、上記クライアントに、上記第2の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び上記第1の証明鍵証明書を削除させる機能を設け、さらに、上記第2の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行う機能を設けるとよい。

#### 【0040】

また、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバ



と通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段として機能させるためのプログラムを含め、その第2の送信手段が、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行うようにし、上記第1の送信手段が、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行うようにしたプログラムも提供する。

#### 【0041】

あるいはまた、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第1の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第2の送信手段として機能させるためのプログラムを含め、上記第1の送信手段の機能を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する機能とし、上記第2の送信手段の機能を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する機能としたプログラムも提供する。

#### 【0042】

また、これらのプログラムにおいて、上記コンピュータを、上記クライアントとは上記サーバを介して通信を行うよう機能させるためのプログラムを含め、そのサーバを、上記第1の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用了認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するサーバとするとよい。

あるいは、上記コンピュータを、上記サーバとは上記クライアントを介して通信を行うよう機能させるためのプログラムを含め、そのクライアントを、上記第2の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用了認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するクライアントとするとよい。

さらに、以上の各プログラムにおいて、上記認証を、SSL又はTLSのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

#### 【発明の効果】

#### 【0043】

以上のようなこの発明のデジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法によれば、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることができる。

また、この発明のプログラムによれば、コンピュータにデジタル証明書管理装置を制御させてこのようなデジタル証明書管理装置の特徴を実現し、同様な効果を得ることができる。

**【発明を実施するための最良の形態】****【0044】**

以下、この発明の好ましい実施の形態を図面を参照して説明する。

**〔第1の実施形態：図1乃至図13〕**

まず、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント及びサーバによって構成される、この発明のデジタル証明書管理システムの第1の実施形態の構成について説明する。図2に、このデジタル証明書管理システムを構成する各装置の、この実施形態の特徴となる部分の機能構成を示す機能ブロック図を示す。図2において、この実施形態の特徴と関連しない部分の図示は省略している。

**【0045】**

図2に示すように、このデジタル証明書管理システムは、証明書管理装置10、サーバ装置30、クライアント装置40によって構成される。

そして、クライアント装置（クライアント）40及びサーバ装置（サーバ）30は、公開鍵暗号とデジタル証明書を用いる認証方式であるSSLによる認証処理によって通信相手を正当な通信相手として認証した場合に、通信を確立させるようにしている。この認証が、互いが互いを認証する相互認証でも一方が他方を認証する片方向認証であってもよいことは、後述する通りである。そして、クライアント装置40が送信した要求に対し、サーバ装置30が必要な処理を行って応答を返すことにより、クライアント・サーバシステムとして機能する。証明書管理装置10は、上記の認証処理に用いるデジタル証明書を発行し、またそのデジタル証明書の管理や更新等を行うための装置であり、CAに相当する。

**【0046】**

なお、実際のシステムにおいては、サーバ装置30がクライアントの機能を併せ持ったり、クライアント装置40がサーバの機能を併せ持ったりすることも考えられる。そして、サーバ装置30がクライアントとして機能して、サーバとして機能するクライアント装置40に要求を送信することもありうるが、このような場合には、後述する第2の実施形態に準ずる動作を行うようにすればよい。従って、ここでは後述するルート鍵更新処理においてサーバとして機能する装置をサーバ装置、クライアントとして機能する装置をクライアント装置と呼ぶものとする。

**【0047】**

このようなデジタル証明書管理システムにおいて、上述のクライアント装置40からサーバ装置30への送信も含め、証明書管理装置10、サーバ装置30、クライアント装置40の各ノードは、RPC（remote procedure call）により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

**【0048】**

すなわち、サーバ装置30又はクライアント装置40では、証明書管理装置10への要求を生成してこれを証明書管理装置10へ引き渡し、この要求に対する応答を取得できる一方で、証明書管理装置10は、クライアント・サーバシステム側への要求を生成してこれをサーバ装置30へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、サーバ装置30にクライアント装置40に対して各種要求を送信させ、クライアント装置40からの応答をサーバ装置30を介して取得することも含まれる。

なお、RPCを実現するために、SOAP（Simple Object Access Protocol）、HTTP（Hyper Text Transfer Protocol）、FTP（File Transfer Protocol）、COM（Component Object Model）、CORBA（Common Object Request Broker Architecture）等の既知のプロトコル（通信規格）、技術、仕様などを利用することができる。

**【0049】**

この送受信のデータ送受モデルを図3の概念図に示す。

(A)は、証明書管理装置10でクライアント装置40に対する要求が発生したケース

である。このケースでは、証明書管理装置 10 が管理装置側要求 a を生成し、これをサーバ装置 30 を経由して受け取ったクライアント装置 40 がこの要求に対する応答 a を返すというモデルになる。なお、(A) では、応答 a だけでなく応答遅延通知 a' を返信するケースが表記されている。これは、クライアント装置 40 が、サーバ装置 30 を経由して管理装置側要求 a を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

なおここでは、サーバ装置 30 からクライアント装置 40 に対して通信を要求することはできないので、サーバ装置 30 からクライアント装置 40 に対して送信すべき要求は、クライアント装置 40 からサーバ装置 30 に対して接続要求があった場合に、これに対する応答として送信することになる。

#### 【0050】

(B) は、クライアント装置 40 で証明書管理装置 10 に対する要求が発生したケースである。このケースでは、クライアント装置 40 がクライアント装置側要求 b を生成し、これをサーバ装置 30 を経由して受け取った証明書管理装置 10 が、当該要求に対する応答 b を返すというモデルになっている。なお、(B) のケースでも、応答を即座に返せないときに応答遅延通知 b' を返すことは (A) のケースと同様である。

#### 【0051】

次に、このデジタル証明書管理システムを構成する各装置の構成と機能についてより詳細に説明する。

図 1 は、図 2 に示した証明書管理装置のハードウェア構成を示すブロック図である。この図に示す通り、証明書管理装置 10 は、CPU 11, ROM 12, RAM 13, HDD 14, 通信インタフェース (I/F) 15 を備え、これらがシステムバス 16 によって接続されている。そして、CPU 11 が ROM 12 や HDD 14 に記憶している各種制御プログラムを実行することによってこの証明書管理装置 10 の動作を制御し、後述するように各手段 (証明鍵更新手段, 第 1 の送信手段, 第 2 の送信手段, その他の手段) として機能させる。

なお、証明書管理装置 10 のハードウェアとしては、適宜公知のコンピュータを採用することができる。もちろん、必要に応じて他のハードウェアを付加してもよい。

#### 【0052】

クライアント・サーバシステムを構成するクライアント装置及びサーバ装置については、装置の遠隔管理、電子商取引等の目的に応じて種々の構成をとることができる。例えば、遠隔管理の場合には、プリンタ、FAX 装置、コピー機、スキャナ、デジタル複合機等の画像処理装置を始め、ネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等の電子装置を被管理装置であるサーバ装置とし、これらの被管理装置から情報を収集したり、コマンドを送って動作させたりするための管理装置をクライアント装置とすることが考えられる。

#### 【0053】

しかし、クライアント装置及びサーバ装置は、少なくともそれぞれ CPU, ROM, RAM, ネットワークを介して外部装置と通信するための通信 I/F、および認証処理に必要な情報を記憶する記憶手段を備え、CPU が ROM 等に記憶した所要の制御プログラムを実行することにより、装置をクライアントあるいはサーバとして機能させることができるものとする。

なお、この通信には、有線、無線を問わず、ネットワークを構築可能な各種通信回線 (通信経路) を採用することができる。証明書管理装置 10 との間の通信についても同様である。

#### 【0054】

図 2 には、上述のように、各装置のこの実施形態の特徴となる部分の機能構成を示している。

まず、証明書管理装置 10 は、証明用鍵作成部 21, 証明書発行部 22, 証明書管理部

23, 証明書更新部24, 通信機能部25を備えている。

証明用鍵作成部21は、デジタル署名の作成に用いる証明用私有鍵であるルート私有鍵と、そのデジタル証明書の正当性を確認するための、ルート私有鍵と対応する証明用公開鍵(証明鍵)であるルート鍵とを作成する証明用鍵作成手段の機能を有する。

#### 【0055】

証明書発行部22は、サーバ装置30とクライアント装置40との間の認証処理に用いる認証情報であるクライアント公開鍵およびサーバ公開鍵にデジタル署名を付して、デジタル証明書であるクライアント公開鍵証明書およびサーバ公開鍵証明書として発行する証明書発行手段の機能を有する。また、クライアント公開鍵、クライアント私有鍵、サーバ公開鍵、サーバ私有鍵の作成及び、ルート鍵にデジタル署名を付したデジタル証明書であるルート鍵証明書の作成も、この証明書発行部22の機能である。

証明書管理部23は、証明書発行部22が発行したデジタル証明書、その作成に用いたルート私有鍵、およびそのルート私有鍵と対応するルート鍵を管理する証明書管理手段の機能を有する。そして、これらの証明書や鍵を、その有効期限や発行先、ID、更新の有無等の情報と共に記憶する。

#### 【0056】

証明書更新部24は、ルート鍵の更新を行う場合に、有効なルート私有鍵の各々について、新たなルート私有鍵(新ルート私有鍵)及びこれと対応する新たなルート鍵(新ルート鍵)を証明用鍵作成部21に作成させ、これらを更新する証明用鍵更新手段の機能を有する。さらに、この更新に当たって、証明書発行部22に新ルート私有鍵を用いてデジタル署名を付した新たなクライアント公開鍵証明書(新クライアント公開鍵証明書)、新たなサーバ公開鍵証明書(新サーバ公開鍵証明書)及び新たなルート鍵証明書(新ルート鍵証明書)を発行させ、通信機能部25によってこれらをサーバ装置30及びクライアント装置40に送信させ、サーバ装置30及びクライアント装置40にこれらの更新を要求させる機能も有する。また、詳細は後述するが、更新に必要な各処理の手順や進捗状況の管理も証明書更新部24が行う。

#### 【0057】

通信機能部25は、ネットワークを介して外部装置と通信する機能を有し、証明書管理部23の指示に応じて必要なデータをサーバ装置30及びクライアント装置40に送信したり、受信したデータを証明書更新部24に渡したりする。

そして、これらの各部の機能は、図1に示したCPU11が所要の制御プログラムを実行して証明書管理装置10の各部の動作を制御することにより実現される。

#### 【0058】

一方、サーバ装置30は、証明書記憶部31, 通信機能部32, サーバ機能部33を備えている。

証明書記憶部31は、SSLによる認証処理に用いる鍵を記憶する機能を有し、例えば相互認証を行う場合には、ルート鍵証明書、サーバ私有鍵、およびサーバ公開鍵証明書を記憶する。

通信機能部32は、ネットワークを介して外部装置と通信する機能を有し、受信したデータをサーバ機能部33に渡し、またサーバ機能部33の指示に従ってデータを外部装置に送信する。

#### 【0059】

サーバ機能部33は、クライアント装置40から受信した要求に対して所要の処理を行って応答を返すサーバとしての機能を有する。また、以下に詳述するが、証明書管理装置10から受信した証明書更新等の要求に対しても、所要の処理を行って応答を返す。

そして、これらの各部の機能は、サーバ装置30のCPUが所要の制御プログラムを実行してサーバ装置30の各部の動作を制御することにより実現される。

#### 【0060】

また、クライアント装置40は、証明書記憶部41, 通信機能部42, クライアント機能部43を備えている。

証明書記憶部 41 は、SSL による認証処理に用いる鍵を記憶する機能を有し、例えば相互認証を行う場合には、ルート鍵証明書、クライアント私有鍵、およびクライアント公開鍵証明書を記憶する。

通信機能部 42 は、ネットワークを介して外部装置と通信する機能を有し、受信したデータをクライアント機能部 43 に渡し、またクライアント機能部 43 の指示に従ってデータを外部装置に送信する。

#### 【0061】

クライアント機能部 43 は、ユーザからの操作、図示しないセンサが検出した状態変化、あるいは図示しないタイマによって計測した所定時間経過等をトリガとして、サーバ装置 30 に対して所要の要求を送信し、サーバ装置 30 からこれに対する応答を受信した場合にはその内容に従った処理を行うクライアントとしての機能を有する。また、以下に詳述するが、応答として証明書管理装置 10 からの証明書更新等の要求を受信した場合には、所要の処理を行って応答を返す。

そして、これらの各部の機能は、クライアント装置 40 の CPU が所要の制御プログラムを実行してクライアント装置 40 の各部の動作を制御することにより実現される。

#### 【0062】

なお、このデジタル証明書管理装置において、証明書管理装置 10 が直接通信可能なのは、クライアント・サーバシステムを構成する装置のうちサーバ装置 30 のみであり、証明書管理装置 10 からクライアント装置 40 に対する要求は、サーバ装置 30 が中継して送るものとする。クライアント装置 40 から証明書管理装置 10 への応答も、同様である。

また、上記のサーバ装置 30 及びクライアント装置 40 には、工場出荷時あるいはそれに順ずる時期、少なくともユーザが認証処理の運用を開始する前に、初めのルート鍵を記憶させておくものとする。このとき、公開鍵証明書及び私有鍵も共に記憶させるようにするとよい。

#### 【0063】

次に、このような基本的な機能を有する図 2 に示したデジタル証明書管理システムにおけるこの実施形態の特徴に関連する処理である、ルート鍵更新処理およびそのために必要な構成について説明する。

なお、以下の説明に用いるシーケンス図に記載するサーバ装置 30 とクライアント装置 40 と間の通信処理に際しては、個々に図示はしていないが、通信の確立前に SSL による認証処理を行い、認証が成功した場合のみ、その SSL によって確保した通信経路でデータの転送を行うものとする。そして、この認証処理に支障を来さないようにルート鍵証明書を更新可能であることが、この実施形態の特徴である。なお、更新に際しての認証は、認証を行おうとする時点で記憶しているルート鍵や公開鍵証明書をを用いて行うことになる。すなわち、更新前は更新前のものを、更新後には更新後のものをを用いて認証を行うことになる。

またここでは、証明書管理装置 10 とサーバ装置 30 との間の通信は、直通回線等の、安全（データの改竄や盗聴がなされないこと）を確保できる通信経路を介して行うものとする。

#### 【0064】

ここで、まず、上述の SSL を用いて認証処理を行う場合の通信手順について説明する。この認証処理としては、互いが互いを認証する相互認証と、一方が他方を認証する片方向認証とが考えられ、各実施形態においてどちらの方式を採用してもよいが、まず、相互認証について説明する。

図 4 に、クライアント装置とサーバ装置とが SSL による相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

図 4 に示すように、SSL による相互認証を行う際には、まずクライアント装置 40 側にルート鍵証明書、クライアント私有鍵、クライアント公開鍵証明書（クライアント証明書）を記憶させておく。クライアント私有鍵は、証明書管理装置 10 がクライアント装置

40に対して発行した私有鍵である。そして、クライアント公開鍵証明書は、その私有鍵と対応する公開鍵に証明書管理装置10がデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、証明書管理装置10がデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。

#### 【0065】

また、サーバ装置30側には、ルート鍵証明書、サーバ私有鍵、サーバ公開鍵証明書（サーバ証明書）を記憶させておく。サーバ私有鍵及びサーバ公開鍵証明書は、証明書管理装置10がサーバ装置30に対して発行した私有鍵及び公開鍵証明書である。ここではクライアント装置40とサーバ装置30に対して同じ証明書管理装置10が同じルート私有鍵を用いて証明書を発行しているものとし、従ってルート鍵証明書はクライアント装置40とサーバ装置30で共通となる。

これらの各鍵や証明書の関係は、背景技術の項で図41を用いて説明した通りである。

#### 【0066】

フローチャートの説明に入る。なお、図4において、2本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。

#### 【0067】

クライアント装置40のCPUは、サーバ装置30に通信を要求する場合、所要の制御プログラムを実行することにより、図4の左側に示すフローチャートの処理を開始する。そして、ステップS11でサーバ装置に対して接続要求を送信する。

一方サーバ装置30のCPUは、この接続要求を受信すると、所要の制御プログラムを実行することにより、図4の右側に示すフローチャートの処理を開始する。そして、ステップS21で第1の乱数を生成し、これをサーバ私有鍵を用いて暗号化する。そして、ステップS22でその暗号化した第1の乱数とサーバ公開鍵証明書とをクライアント装置40に送信する。

#### 【0068】

クライアント装置40側では、これを受信すると、ステップS12でルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認する。これには、損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置30が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップS13で、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて第1の乱数を復号化する。ここで復号化が成功すれば、第1の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置30から受信したものと確認できる。そして、サーバ装置30を正当な通信相手として認証する。

#### 【0069】

その後、ステップS14でこれとは別に第2の乱数及び第3の乱数を生成する。そして、ステップS15で第2の乱数をクライアント私有鍵を用いて暗号化し、第3の乱数をサーバ公開鍵を用いて暗号化し、ステップS16でこれらをクライアント公開鍵証明書と共にサーバ装置30に送信する。第3の乱数の暗号化は、サーバ装置30以外の装置に乱数を知られないようにするために行うものである。

#### 【0070】

サーバ装置30側では、これを受信すると、ステップS23でルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認する。これにも、ステップS12の場合と同様、クライアント装置40が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップS24で、受信したクライアント公開鍵証明書に含まれるクライアント公開鍵を用いて第2の乱数を復号化する。ここで復号化が成功すれば、第2の乱数は

確かにクライアント公開鍵証明書の発行対象であるクライアント装置 40 から受信したものと確認できる。そして、クライアント装置 40 を正当な通信相手として認証する。

#### 【0071】

その後、ステップ S 25 でサーバ私有鍵を用いて第 3 の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第 1 乃至第 3 の乱数が共有されたことになる。そして、少なくとも第 3 の乱数は、生成したクライアント装置 40 と、サーバ私有鍵を持つサーバ装置 30 以外の装置が知ることはない。ここまでの処理が成功すると、ステップ S 26 でクライアント装置 40 に対して認証成功の応答を返す。

#### 【0072】

クライアント装置 40 側では、これを受信すると、ステップ S 17 で第 1 乃至第 3 の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。サーバ装置 30 側でも、ステップ S 27 で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップ S 17 又は S 27 で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

このような処理を行うことにより、クライアント装置 40 とサーバ装置 30 が互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。

#### 【0073】

なお、片方向認証の場合、図 4 に示した処理は、図 5 に示すように簡略化することができる。すなわち、この場合には、第 2 の乱数をクライアント私有鍵で暗号化し、公開鍵証明書 A を通信装置 B に送信することは必須ではない。この場合、サーバ装置 30 側のステップ S 23 及び S 24 の処理は不要になる。このようにすると、サーバ装置 30 がクライアント装置 40 を認証することはできないが、クライアント装置 40 がサーバ装置 30 を認証するだけでよい場合にはこの処理で十分である。

そしてこの場合には、クライアント装置 40 に記憶させるのはルート鍵証明書のみでよく、クライアント私有鍵及びクライアント公開鍵証明書は不要である。また、サーバ装置 30 にはルート鍵証明書を記憶させる必要はない。従ってこの場合、以下に説明する各ルート鍵証明書の更新処理も、クライアント装置 40 のルート鍵証明書とサーバ装置 30 のサーバ公開鍵証明書のみを更新する処理に簡略化することが可能である。

#### 【0074】

次に、ルート鍵証明書の更新処理の説明に移るが、ここで説明するルート鍵更新処理は、この発明のデジタル証明書管理方法の第 1 の実施形態に係る処理であり、図 6 乃至図 12 のシーケンス図に示す処理を、図 13 のフローチャートに示す順番で実行するものである。そこで、まず図 6 乃至図 12 の各シーケンス図に示す処理の内容を説明してから、図 13 を用いてその実行順について説明する。以下の各図に示す処理は、証明書管理装置 10、サーバ装置 30、クライアント装置 40 の各 CPU が、所要の制御プログラムを実行することによって行うものである。

#### 【0075】

まず図 6 のシーケンス図に処理 S としてルート鍵証明書作成処理を示す。

この処理においては、証明書管理装置 10 は、ステップ S 101 で、有効なルート私有鍵について、新たなルート私有鍵とルート鍵のペアを作成する。ここで、「有効な」ルート私有鍵とは、その時点でクライアント・サーバシステムにおける認証処理に使用中のルート私有鍵という意味であり、より正確には、そのルート私有鍵を用いてデジタル署名を付した証明書が、認証処理に用いられる状態でサーバ装置 30 又はクライアント装置 40 に記憶されているものをいうものとする。過去に作成した私有鍵が有効か否かは、証明書管理部 23 に記憶している公開鍵証明書及びルート鍵証明書の有効期限やその更新の有無の情報や、証明書に含まれる、デジタル署名に使用したルート私有鍵の識別情報等の情報を基に判断することができる。また、新たな鍵と置き換えられるべきそれまでの鍵を、「従前の」鍵と呼ぶことにする。証明書についても同様である。

そして、ステップ S 102 で、ステップ S 101 で作成した新ルート鍵に従前のルート



私有鍵を用いたデジタル署名を付し、第1の証明鍵証明書である配布用ルート鍵証明書を作成する。

以上がルート鍵証明書作成処理である。

#### 【0076】

次に、図7のシーケンス図に処理1としてサーバ装置のルート鍵証明書記憶処理を示す。

この処理においては、まずステップS111で、証明書管理装置10がサーバ装置30に対して、図6のステップS102で作成した配布用ルート鍵証明書と共に、その更新要求を送信する。この処理において、証明書管理装置10のCPU11が第2の送信手段として機能する。

#### 【0077】

サーバ装置30は、この要求を受け取ると、ステップS112で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認する。上述のように、配布用ルート鍵証明書には、従前のルート私有鍵を用いたデジタル署名を付しているのので、従前のルート鍵を用いてその内容を復号化し、確かに証明書管理装置10によって発行されたものであることを確認できる。また、このとき、背景技術の項で図41を用いて説明したようにルート鍵が損傷や改竄等を受けていないことも確認できる。従って、このような配布用ルート鍵証明書を用いることにより、受け取ったルート鍵の正当性を人手によらず確認できることになる。

そして、これが確認できると、次のステップS113で配布用ルート鍵証明書を証明書記憶部31に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。従って、証明書記憶部31には2つのルート鍵証明書が記憶された状態となる。

#### 【0078】

この状態で認証処理を行う場合、受信した公開鍵証明書の正当性を確認する際には、2つのルート鍵証明書を順次用いて確認を試み、どちらかのルート鍵証明書を用いて確認が成功すれば、正当性が確認できたものとする。従って、新旧どちらのルート私有鍵を用いてデジタル署名を付したデジタル証明書であっても、その正当性を確認することができる。なお、配布用ルート鍵証明書を認証処理に使用する際の、ルート鍵に破損や改竄がないことの確認は、従前のルート鍵証明書を用いて行うことができる。これらのステップS112及びS113において、サーバ装置30のCPUが第2のサーバ側更新手段として機能する。

サーバ装置30はその後、ステップS114で証明書管理装置10に対して更新要求に対する応答として結果通知を返し、配布用ルート鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。なお、この結果通知は、少なくともサーバ装置30が配布用ルート鍵証明書を受信したことを示す情報である。以下の結果通知も同様な意味を持つものとする。

以上がサーバ装置のルート鍵証明書記憶処理である。

#### 【0079】

次に、図8のシーケンス図に処理2としてクライアント装置のルート鍵証明書記憶処理を示す。

この処理においては、まずステップS121で、証明書管理装置10がサーバ装置30に対して、図6のステップS102で作成した配布用ルート鍵証明書と共に、その更新要求をクライアント装置40に送信するよう要求する更新要求送信要求を送信する。サーバ装置30は、これに応じてクライアント装置40に対して配布用ルート鍵証明書とその更新要求とを送信するのであるが、サーバ装置30側から送信要求を行うことはできない。そこで、クライアント装置40が所定のタイミングで定期的にサーバ装置30に対して通信要求を送信するようにし(S122)、これに対する応答として配布用ルート鍵証明書とその更新要求とを送信するようにしている(S123)。

#### 【0080】

なお、クライアント装置40がサーバ装置30に対する通信要求をHTTPリクエスト



として送信し、サーバ装置 30 からクライアント装置 40 に対して送信する要求やデータをこれに対する応答である HTTP レスポンスとして送信するようにするとよい。このようにすれば、クライアント装置 40 がファイアウォールの内側に設置されている場合でも、これを越えてサーバ装置 30 からクライアント装置 40 にデータを転送することができる。

#### 【0081】

ファイアウォールを越える手段はこれに限られるものではなく、例えば、SMTP (Simple Mail Transfer Protocol) を利用して、送信したいデータを記載あるいは添付したメールを送信することも考えられる。ただし、信頼性の面では HTTP が優れている。

以上の処理により、証明書管理装置 10 からクライアント装置 40 に、サーバ装置 30 を介して配布用ルート鍵証明書とその更新要求とが送信されることになり、ステップ S121 の処理においては、証明書管理装置 10 の CPU 11 が第 1 の送信手段として機能する。

#### 【0082】

クライアント装置 40 は、この要求を受け取ると、ステップ S124 で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップ S125 で配布用ルート鍵証明書を証明書記憶部 41 に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。これらの確認と記憶の詳細については、図 7 のステップ S112 及び S113 の場合と同様であり、これらのステップにおいて、クライアント装置 40 の CPU が第 2 のクライアント側更新手段として機能する。

クライアント装置 40 はその後、ステップ S126 で証明書管理装置 10 に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置 30 に対して送信し、サーバ装置 30 がステップ S127 で証明書管理装置に対して送信する。

以上がクライアント装置のルート鍵証明書記憶処理である。

#### 【0083】

次に、図 9 のシーケンス図に処理 3 としてクライアント装置の公開鍵証明書記憶処理を示す。

この処理においてはまずステップ S131 で、証明書管理装置 10 が、クライアント装置 40 に対して発行してあるクライアント公開鍵に、新ルート私有鍵を用いたデジタル署名を付して新クライアント公開鍵証明書を作成する。なお、クライアント私有鍵は更新しないので、クライアント公開鍵自体も更新する必要はない。

#### 【0084】

そしてステップ S132 で、証明書管理装置 10 がサーバ装置 30 に対して、ステップ S131 で作成した新クライアント公開鍵証明書と共に、その更新要求をクライアント装置 40 に送信するよう要求する更新要求送信要求を送信する。サーバ装置 30 は、これに応じて、図 8 のステップ S122 及び S123 の場合と同様に、クライアント装置 40 からの通信要求 (S133) に対する応答として新クライアント公開鍵証明書とその更新要求とを送信するようにしている (S134)。

以上の処理により、証明書管理装置 10 からクライアント装置 40 にサーバ装置 30 を介して新クライアント公開鍵証明書とその更新要求とが送信されることになり、ステップ S132 の処理においては、証明書管理装置 10 の CPU 11 が第 1 の送信手段として機能する。

#### 【0085】

クライアント装置 40 は、この要求を受け取るとステップ S135 で、図 8 のステップ S125 で記憶した配布用ルート鍵証明書を用いて新クライアント公開鍵証明書の正当性を確認する。上述のように、新クライアント公開鍵証明書には、新ルート私有鍵を用いたデジタル署名を付しているため、配布用ルート鍵証明書に含まれる新ルート鍵を用いてその内容を復号化し、確かに証明書管理装置 10 によってクライアント装置 40 に対して発行されたものであることを確認できる。そして、これが確認できると、次のステップ S136 で新クライアント公開鍵証明書を証明書記憶部 41 に記憶する。これらのステップ S

135及びS136において、クライアント装置40のCPUが第1のクライアント側更新手段として機能する。

#### 【0086】

このとき、まだ従前のクライアント公開鍵証明書は消去しない。従って、証明書記憶部41には2つのクライアント公開鍵証明書が記憶された状態となる。この状態で認証処理を行い、通信相手に対して公開鍵証明書を送信する場合には、まず新公開鍵証明書を送信するものとする。

この場合、通信相手が既に新ルート鍵を（配布用ルート鍵証明書又は後述する新ルート鍵証明書として）記憶していれば、新公開鍵証明書のデジタル署名を復号化できるので、問題なく認証を受けることができる。一方、通信相手がまた新ルート鍵を記憶していない場合には、新公開鍵証明書のデジタル署名を復号化できず、認証が失敗した旨の応答を受けることになる。しかしこの場合でも、再度通信を要求し、この際に従前の公開鍵証明書を送信するようにすれば、従前のルート鍵によってそこに付されたデジタル署名を復号化できるので、問題なく認証を受けることができる。

#### 【0087】

従って、2つの公開鍵証明書を記憶しておけば、通信相手が新ルート鍵を記憶していない場合に多少のオーバーヘッドが生じることはあるが、問題なく認証処理を行うことができる。なお、2つの公開鍵証明書に含まれる公開鍵本体は同じものであるので、クライアント私有鍵を用いて暗号化したデータの復号化は、どちらの公開鍵証明書を用いた場合でも同じように行うことができる。

クライアント装置40はその後、ステップS137で証明書管理装置10に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置30に対して送信し、サーバ装置30がステップS138で証明書管理装置に対して送信する。

以上がクライアント装置の公開鍵証明書記憶処理である。

#### 【0088】

次に、図10のシーケンス図に処理4としてサーバ装置の公開鍵証明書記憶処理を示す。

この処理においてはまずステップS141で、証明書管理装置10が、クライアント装置40に対して発行してあるサーバ公開鍵に、新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成する。サーバ公開鍵自体の更新が不要であることは、上述のクライアント公開鍵の場合と同様である。

そしてステップS142で、証明書管理装置10がサーバ装置30に対して、新サーバ公開鍵証明書と共にその更新要求を送信する。この処理において、証明書管理装置10のCPU11が第2の送信手段として機能する。

#### 【0089】

サーバ装置30は、この要求を受け取るとステップS143で、図7のステップS113で記憶した配布用ルート鍵証明書を用いて新公開鍵証明書の正当性を確認する。この点については、図9のステップS135の場合と同様である。そして、これが確認できると、次のステップS144で新サーバ公開鍵証明書を証明書記憶部41に記憶し、従前のサーバ公開鍵証明書と置き換える。これらのステップS143及びS144において、サーバ装置30のCPUが第1のサーバ側更新手段として機能する。

#### 【0090】

ところで、サーバ装置30の場合には、クライアント装置40の場合と異なり、新公開鍵証明書を記憶させる場合に従前のものに追加するのではなくこれと置き換える必要があるものの、ここでこの点について説明する。

サーバ装置30の場合には、クライアント装置40から接続要求があった場合に公開鍵証明書をクライアント装置40に送信するのであるが、サーバ公開鍵証明書を複数記憶していたとすると、送信毎にそのうちいずれかを選択して送信することになる。そして、クライアント装置40側でデジタル証明書を復号化できないようなサーバ公開鍵証明書を送信してしまった場合には、認証は失敗することになる。例えば、クライアント装置40が

新ルート鍵を記憶する前に新サーバ公開鍵証明書を送信した場合等である。

【0091】

たとえ失敗したとしても、次に接続要求があった場合にもう一方のサーバ公開鍵証明書を送信すればよいという考え方もあるが、不特定多数のクライアント装置から任意のタイミングで接続要求を受け得るサーバ装置の場合、クライアント装置毎に送信すべきサーバ公開鍵証明書を選択することは、現実的ではない。また、クライアント装置がどのような装置であるかは、サーバ装置側では認証が済むまで通常わからないので、最初に送信するサーバ公開鍵証明書を適切に選択することも困難である。従って、サーバ装置にはサーバ公開鍵証明書を1つだけ記憶させ、クライアント装置から接続要求を受けた場合には常にこれを送信するようにする必要があるのである。

【0092】

従って、サーバ装置30では新サーバ公開鍵証明書を記憶させた時点で従前のサーバ公開鍵証明書は削除してしまうので、クライアント装置40に新ルート鍵を記憶させる前にこれを行ってしまうと、クライアント装置側でサーバ公開鍵証明書のデジタル署名を復号化できなくなり、認証処理を行えなくなってしまう。そこで、サーバ装置30の公開鍵証明書記憶処理は、クライアント装置のルート鍵証明書記憶処理の完了後に行う必要がある。

以上のようなステップS144の終了後、サーバ装置30はステップS145で証明書管理装置10に対して更新要求に対する応答として結果通知を返し、新サーバ公開鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。

以上がサーバ装置の公開鍵証明書記憶処理である。

【0093】

次に、図11のシーケンス図に処理5としてサーバ装置のルート鍵証明書書き換え処理を示す。

この処理においてはまずステップS151で、証明書管理装置10が、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第2の証明鍵証明書として新ルート鍵証明書を作成する。そして、ステップS152で証明書管理装置10がサーバ装置30に対して、新ルート鍵証明書と共にその更新要求を送信する。この処理においても、証明書管理装置10のCPU11が第2の送信手段として機能する。

【0094】

サーバ装置30は、この要求を受け取ると、ステップS153で配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。上述のように、新ルート鍵証明書には、新ルート私有鍵を用いたデジタル署名を付しているので、配布用ルート鍵証明書に含まれる新ルート鍵を用いてその内容を復号化し、確かに証明書管理装置10によって発行されたものであることを確認できる。

そして、これが確認できると、次のステップS154で新ルート鍵証明書を証明書記憶部31に記憶する。そして、配布用ルート鍵証明書及び従前のルート鍵証明書を削除して廃棄し、ルート鍵証明書を新たなものに書き換えてしまう。このようにすると、従前のルート私有鍵を用いてデジタル署名を付したデジタル証明書は復号化できなくなってしまうが、クライアント装置40に新クライアント公開鍵証明書を記憶させた後であれば、クライアント装置40から送られてくる公開鍵証明書の確認には支障がないので、認証処理に支障を来すことはない。

【0095】

サーバ装置30はその後、ステップS155で証明書管理装置10に対して更新要求に対する応答として結果通知を返し、新ルート鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。

以上がサーバ装置のルート鍵証明書書き換え処理である。

【0096】

次に、図12のシーケンス図に処理6としてクライアント装置のルート鍵証明書書き換え処理を示す。

この処理においてはまずステップS161で、証明書管理装置10が、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第2の証明鍵証明書として新ルート鍵証明書を作成する。これは、図11のステップS151で作成するものと同じであるので、ここで作成したものを流用してもよい。逆に図11のステップS151で、このステップS161で作成したものを流用してもよい。

#### 【0097】

そしてステップS162で、証明書管理装置10がサーバ装置30に対して、ステップS161で作成した新ルート鍵証明書と共に、その更新要求をクライアント装置40に送信するように要求する更新要求送信要求を送信する。サーバ装置30は、これに応じて、図8のステップS122及びS123の場合と同様に、クライアント装置40からの通信要求(S163)に対する応答として新ルート鍵証明書とその更新要求とを送信するようにしている(S164)。

以上の処理により、証明書管理装置10からクライアント装置40にサーバ装置30を介して新ルート鍵証明書とその更新要求とが送信されることになり、ステップS162の処理においても、証明書管理装置10のCPU11が第1の送信手段として機能する。

#### 【0098】

クライアント装置40は、この要求を受け取ると、ステップS165で配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップS166で新ルート鍵証明書を証明書記憶部41に記憶する。そして、配布用ルート鍵証明書及び従前のルート鍵証明書を削除して廃棄し、ルート鍵証明書を新たなものに書き換えてしまう。これらの処理については、図11のステップS153及びS154の場合と同様である。ただし、クライアント装置40への新クライアント公開鍵証明書の記憶が済んでいれば、ステップS166で従前のクライアント公開鍵証明書も同時に廃棄してしまってもよい。

#### 【0099】

クライアント装置40はその後、ステップS167で証明書管理装置10に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置30に対して送信し、サーバ装置30がステップS168で証明書管理装置に対して送信する。

以上がクライアント装置のルート鍵証明書書き換え処理である。

#### 【0100】

以上の図6乃至図12に示した各処理の実行タイミングは、証明書管理装置10の証明書更新部24が、図13に示すフローチャートに従って管理する。すなわち、ルート鍵の更新事由を検出した場合に、図13のフローチャートに示す処理を開始し、まず図6に示した処理Sを実行し、その後処理1乃至処理6を実行する。なお、ルート鍵の更新事由としては、所定の有効期限の到来、管理者の指示等が考えられる。管理者が更新の指示を行う場合としては、ルート私有鍵の第3者への漏洩が判明した場合等が考えられる。

また、図13において、矢印の先の処理は、矢印の根元側の処理が全て完了してから開始する。破線で示した矢印については、その条件は必須ではないが考慮した方が好ましいということを示す。

#### 【0101】

具体的には、処理1及び処理2は処理Sの完了後に開始する。処理3は、処理2の完了後に開始するが、処理1も完了した後に開始する方が好ましい。処理4は、処理1及び処理2の完了後に開始する。処理5は、処理1及び処理3の完了後に開始する。処理6は、処理2及び処理4の完了後に開始する。そして、処理3乃至6が全て完了した時点で、ルート鍵及び公開鍵証明書の更新が終了したことになる。

なお、各処理は、更新要求に対する更新成功の応答を受け取った場合に完了したものとしてすることができる。この応答が、更新すべき証明書を受信した旨を示す情報も含むことは、上述した通りである。更新失敗の応答を受け取った場合や処理がタイムアウトした場合には、再度同じ処理を試みるとよいが、所定回数続けて失敗した場合には更新処理全体が失敗したものとするとよい。

## 【0102】

また、ここでは、図7等にしたように、証明書管理装置10がサーバ装置30に更新要求を送信した場合、サーバ装置30が受信した証明書等の記憶を完了してから結果通知を返す例について説明した。しかし、図14に示すように、サーバ装置30が更新要求を受信した場合に直ちに受信応答を返す(S111')ようにしてもよい。このようにした場合、ステップS111'の受信応答が、証明書管理装置10が送信した更新要求及び配布用ルート鍵証明書を正常に受信した旨の情報となる。また、ステップS114の結果通知は、更新の成否やその原因等を伝える情報となる。そして、この結果通知に対しても、証明書管理装置10が受信応答を返す(S114')ようにするとよい。このようにすれば、サーバ装置30側でも、結果通知が正常に証明書管理装置10に受信されたことが把握できる。

## 【0103】

また、サーバ装置30とクライアント装置40との間の通信についても、同様な手順とし、何らかの要求を受信した場合に、その送信元に対して直ちに受信応答を返し、結果通知についても、これを受信した場合にその送信元に対して直ちに受信応答を返すようにするとよい。図8に示したシーケンスに上記のような考え方を採り入れたシーケンスを図15に示す。

なお、ステップS123'での受信応答が、クライアント装置40が配布用ルート鍵証明書及び更新要求を受信した旨の情報となるが、図8に示したシーケンスに単に上記の考え方を採り入れたシーケンスでは、この情報はサーバ装置30がステップS127の結果通知を行うまで証明書管理装置10には伝わらない。

そこで、図15に破線で示したように、サーバ装置30が、クライアント装置40からの受信応答があった後、送信の成否のみを送信結果通知として証明書管理装置10へ通知するようにしてもよい。このようにすれば、クライアント装置40への送信の成否を速やかに証明書管理装置10に伝えることができる。

## 【0104】

また、以上のように結果通知を行うようにした場合、図13を用いて説明したような各処理の実行タイミング管理において、証明書等の送信先から受信応答があった場合に、送信先において証明書の記憶や設定は滞りなく進行するであろうという予測の下に処理を先の段階に進めてしまうことも可能である。具体的には、処理1が全て完了しなくても、図14のステップS111'に示したような受信応答があった場合に処理1が完了したものとみなして処理4の開始時期を決定するようにしてもよい。また、処理2が全て完了しなくても、図15のステップSAに示したような送信結果通知があった場合に処理2が完了したものとみなして処理4の開始時期を決定するようにしてもよい。

また、ここでは、図14及び図15に、それぞれ図7及び図8のシーケンスの変形例を示したのみであるが、以上のような考え方は、以降の実施例及び変形例に示すものも含め、全ての処理及びシーケンスに適用可能なものである。

## 【0105】

以上のようなタイミング管理に基づき、ルート鍵更新処理を図13に示す手順で行う場合、サーバ装置30とクライアント装置40とは処理のどの時点であってもSSLによる認証処理を行うことができるので、このように更新処理が途中で中断してしまっても、サーバ装置30とクライアント装置40との間の通信に大きな支障はない。従って、更新処理が失敗した場合に時間をかけて失敗の原因を特定した上で改めて更新処理を行っても、特に大きな問題はない。以後の各実施形態についても同様である。

## 【0106】

このデジタル証明書管理システムにおいては、ルート鍵更新処理をこのような手順で行うことにより、サーバ装置30とクライアント装置40との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。また、従前の(更新前の)ルート鍵や公開鍵証明書を用いた認証を行ってSSLによる通信経路を確保し、その通信経路で更新用の新ルート鍵や新公開鍵証明書を送信することができる。また、更新終了

後は、その新ルート鍵や新公開鍵証明書を用いた認証を行ってSSLによる通信経路を確保できる状態にすることができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してSSLによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。この点も、以後の各実施形態についても同様である。

#### 【0107】

また、証明書管理装置10とサーバ装置30との間には、これとは別の安全な通信経路を設ける必要があるが、これは期限切れ等に伴う公開鍵証明書の更新のような、通常必要な処理に使用するものと共通の通信経路でよい。また、このような通信経路は証明書管理装置10と1つの装置のみとの間に設ければよいので、特に大きな負担にはならない。証明書管理装置10とサーバ装置30とが物理的に近接している場合には専用ケーブルで結ぶ等してこのような経路を設けることは容易であり、この実施形態はこのような場合に好ましいものであると言える。

#### 【0108】

図13に示す処理手順において、この実施形態の特徴となるのは、まず、処理4（サーバ装置の公開鍵証明書記憶処理）を処理2（クライアント装置のルート鍵証明書記憶処理）の後で、すなわちクライアント装置40から配布用ルート鍵証明書を受信した旨の応答があった後で実行する点である。

処理4の説明において上述したように、サーバ装置30については公開鍵証明書を同時に2つ記憶させると不都合が生じるので、新サーバ公開鍵証明書を記憶させる際には従前のものを廃棄する必要があるのであるが、このような書き換えを行ってしまっても、クライアント装置40に新ルート鍵を記憶させた後であれば、認証処理に支障が生じることがない。

#### 【0109】

また、処理3（クライアント装置の公開鍵証明書記憶処理）を処理1（サーバ装置のルート鍵証明書記憶処理）の後で、すなわちサーバ装置30から配布用ルート鍵証明書を記憶した旨の応答があった後で実行するようにするとよい。

処理3の説明で上述したように、クライアント装置40に新クライアント公開鍵証明書を記憶させた時点でサーバ装置30に新ルート鍵が記憶されていないと、サーバ装置30に新ルート鍵が記憶されるまで通信にオーバーヘッドが生じ、効率が悪くなってしまうためである。

#### 【0110】

処理5と処理6については、これらは必須の処理ではないが、従前のルート鍵証明書や公開鍵証明書をいつまでも記憶させておくとすると、記憶容量を無駄に消費することになる。鍵や証明書の記憶には、信頼性の高い記憶手段を用いることが好ましく、従って容量当たりのコストが高いため、この点は大きな問題になる。また、配布用ルート鍵証明書は、自己署名形式でないため、使用する際に従前のルート鍵証明書を参照する必要があり、処理効率が悪い。そこで、処理5と処理6を行って、ルート鍵証明書を自己署名形式のものにすると共に、従前の証明書を廃棄するようにするとよい。

#### 【0111】

ルート鍵証明書を自己署名形式のものに書き換えるだけであれば、配布用ルート鍵証明書を記憶させた直後に、例えば処理5の場合には処理1の完了直後に行ってもよいのであるが、この時点では必ずしも従前のルート鍵証明書を廃棄できない。そして、この削除タイミングはサーバ装置30側では決定することができないので、処理3の終了後に再度従前のルート鍵証明書を廃棄する要求を行う必要が生じてしまう。従って、処理1と処理3の完了後に処理5を行うことが、処理の簡略化の点から好ましい。処理6についても、同様の理由から処理2と処理4の完了後に行うことが好ましい。

#### 【0112】

なお、ルート鍵は一旦記憶してしまえば一般に外部に送信する必要はないので、その後

の破損や改竄は考えにくいことから、ルート鍵証明書ではなく、鍵部分のみを記憶することとも考えられる。このような場合には、配布用ルート鍵証明書に含まれる新ルート鍵を記憶してしまえばよいので、証明書管理装置 10 から新ルート鍵証明書を別途送信する必要はない。そこで、このような場合、処理 5、処理 6 においては、新ルート鍵証明書を送信せず、従前のルート鍵の廃棄のみを要求するようにすればよい。また、ルート鍵を使用する際に、デジタル署名の確認を行わないようにする場合についても同様である。

#### 【0113】

また、この実施形態において、サーバ装置 30 からクライアント装置 40 への送信は、クライアント装置 40 からの通信要求に対する応答として行う例について説明したが、サーバ装置 30 がクライアントとしても機能できるようにし、クライアント装置 40 がサーバとしても機能できるようにし、これらの機能によって、サーバ装置 30 からクライアント装置 40 へデータや要求を直接送信できるようにしてもよい。このような場合は、クライアント装置 40 による通信要求は不要である。この点は、以下の実施形態においても同様である。

#### 【0114】

〔第 2 の実施形態：図 16 乃至図 23〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第 2 の実施形態の構成について説明する。

このデジタル証明書管理システムを構成する各装置の、この実施形態の特徴となる部分の機能構成を、図 2 と対応する図 16 の機能ブロック図に示す。この図において、図 2 と対応する部分には同一の符号を付している。

#### 【0115】

この図からわかるように、このデジタル証明書管理システムにおいてはまず、証明書管理装置 10 をクライアント・サーバシステムを構成する装置のうちクライアント装置 40 のみと直接通信可能とし、証明書管理装置 10 からサーバ装置 30 に対する要求は、クライアント装置 40 が中継して送るものとした点が第 1 の実施形態と異なる。

また、クライアント装置 40 にもサーバ機能部 44 を設けた点も、第 1 の実施形態の場合と異なるが、このサーバ機能部 44 は、受信した要求に対して所要の処理を行って応答を返すサーバとしての機能を有し、証明書管理装置 10 との通信のために設けたものである。クライアント装置 40 がクライアント機能部 43 しか有しないとすると、証明書管理装置 10 からクライアント装置 40 にデータや要求等を送信する場合に、クライアント装置 40 からの通信要求を待つ必要が生じてしまう。

#### 【0116】

しかし、ルート鍵の更新処理は頻繁に行われるものではなく、例えば年に 1 回程度であるので、このためにクライアント装置 40 が証明書管理装置 10 に対して定期的に通信要求を行うとすると、ほとんどの通信が無駄になることになる。そこで、クライアント装置 40 にサーバ機能部 44 を設け、証明書管理装置 10 側から通信を要求できるようにしたものである。このサーバ機能部 44 の機能も、クライアント装置 40 の CPU が所要の制御プログラムを実行してクライアント装置 40 の各部の動作を制御することにより実現されるものである。

#### 【0117】

ただし、クライアント・サーバシステムを構成するサーバ装置 30 との関係においては、クライアント装置 40 は常にクライアントとして機能する。従って、証明書管理装置 10 からサーバ装置 30 への通信を仲介する場合には、通信機能部 42 が証明書管理装置 10 から受信したデータや要求を、サーバ機能部 44 が受け取り、これをクライアント機能部 43 に渡して、クライアント機能部 43 の指示に基づいてサーバ装置 30 に対する通信を要求してサーバ装置 30 に送信することになる。サーバ装置 30 からの応答を証明書管理装置 10 に返す場合には、この逆の処理となる。

#### 【0118】



これらの変更に伴ってルート鍵更新処理のシーケンスは変更されるが、それ以外の点については第1の実施形態と同様であるので、説明を省略する。

なおここでも、証明書管理装置10とクライアント装置40との間の通信は、直通回線等の、安全を確保できる通信経路を介して行うものとする。ただし、この実施形態の場合には、証明書管理装置10とクライアント装置40との間の通信にSSLを用いることも可能であるが、この場合の構成については変形例として後述する。

#### 【0119】

このデジタル証明書管理システムにおけるルート鍵更新動作は、この発明のデジタル証明書管理方法の第2の実施形態に係る動作であり、図17乃至図22のシーケンス図に示す処理及び図6を用いて上述した処理Sを、図23のフローチャートに示す順番で実行するものである。そこで、まず図17乃至図22の各シーケンス図に示す処理の内容を説明してから、図22を用いてその実行順について説明する。以下の各図に示す処理は、証明書管理装置10、サーバ装置30、クライアント装置40の各CPUが、所要の制御プログラムを実行することによって行うものである。

#### 【0120】

まず、図17のシーケンス図に処理11としてサーバ装置のルート鍵証明書記憶処理を示す。

この処理は、図7に示した処理1と同じ目的の処理であるが、ここでは証明書管理装置10と直接通信する装置がクライアント装置40であるため、手順が若干異なるものとなっている。

#### 【0121】

すなわち、まずステップS211で、証明書管理装置10がクライアント装置40に対して、図6のステップS102で作成した配布用ルート鍵証明書と共に、その更新要求をサーバ装置30に送信するよう要求する更新要求送信要求を送信する。そしてクライアント装置40は、これに応じてサーバ装置30に対して配布用ルート鍵証明書とその更新要求とを送信する(S212)。クライアント装置40はサーバ装置30に対して通信を要求できるので、図7の場合のように通信要求を待つ必要はない。

以上の処理により、証明書管理装置10からサーバ装置30にクライアント装置40を介して配布用ルート鍵証明書とその更新要求とが送信されることになり、ステップS211の処理においては、証明書管理装置10のCPU11が第2の送信手段として機能する。

#### 【0122】

サーバ装置30は、ステップS212で送信されてきた更新要求を受け取ると、ステップS213で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると、次のステップS214で配布用ルート鍵証明書を証明書記憶部31に記憶する。これらの処理は、図7のステップS112及びS113の処理と全く同じである。

#### 【0123】

サーバ装置30はその後、ステップS215で証明書管理装置10に対して更新要求に対する応答として結果通知を返すが、これはまずクライアント装置40に対して送信し、クライアント装置40がステップS216で証明書管理装置に対して送信する。なお、この結果通知は、クライアント装置40から受信した更新要求に対する応答として送信することができるので、クライアント装置40からの通信要求を待つ必要はない。

以上がこの実施形態におけるサーバ装置のルート鍵証明書記憶処理である。

#### 【0124】

次に、図18のシーケンス図に処理12としてクライアント装置のルート鍵証明書記憶処理を示す。

この処理は、図8に示した処理2と同じ目的の処理であるが、処理11の場合と同様に手順が若干異なるものとなっている。

この処理においては、まずステップS221で、証明書管理装置10がクライアント装



置 40 に対して、図 6 のステップ S 102 で作成した配布用ルート鍵証明書とその更新要求を送信する。この処理において、証明書管理装置 10 の CPU 11 が第 1 の送信手段として機能する。

#### 【0125】

クライアント装置 40 は、この要求を受け取ると、ステップ S 124 で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると、次のステップ S 125 で配布用ルート鍵証明書を証明書記憶部 41 に記憶する。これらの処理は、図 8 のステップ S 124 及び S 125 の処理と全く同じである。

クライアント装置 40 はその後、ステップ S 224 で証明書管理装置 10 に対して更新要求に対する応答として結果通知を返す。

以上がこの実施形態におけるクライアント装置のルート鍵証明書記憶処理である。

#### 【0126】

以下、図 19 に処理 13 としてクライアント装置の公開鍵証明書記憶処理を、図 20 に処理 14 としてサーバ装置の公開鍵証明書記憶処理を、図 21 に処理 15 としてサーバ装置のルート鍵証明書書き換え処理を、図 22 に処理 16 としてクライアント装置のルート鍵証明書書き換え処理をそれぞれ示すが、これらは、第 1 の実施形態で図 9 乃至図 12 を用いてそれぞれ説明した処理 3 乃至処理 6 と同じ目的の処理であり、証明書管理装置 10 と直接通信する装置がクライアント装置 40 であることに伴って、処理 11 及び処理 12 の場合と同様に通信手順を若干変更したのみである。そこで、これらの処理についての説明は省略する。

#### 【0127】

また、以上の図 17 乃至図 22 に示した各処理及び図 6 に示した処理 S の実行タイミングは、証明書管理装置 10 の証明書更新部 24 が図 23 に示すフローチャートに従って管理する。すなわち、ルート鍵の更新を行う場合には、まず図 6 に示した処理 S を実行し、その後処理 11 乃至処理 16 を実行する。

図 23 の記載から明らかなように、この第 2 の実施形態におけるルート鍵更新処理は、図 13 に示した第 1 の実施形態の場合と対応する処理を、同様な順序で行うものである。そして、このことによる効果も、第 1 の実施形態の場合と同様である。

#### 【0128】

すなわち、この第 2 の実施形態のデジタル証明書管理システムにおいては、ルート鍵更新処理をこのような手順で行うことにより、証明書管理装置 10 がクライアント・サーバシステムを構成する装置のうちクライアント装置 40 のみと通信可能な場合でも、第 1 の実施形態の場合と同様に、サーバ装置 30 とクライアント装置 40 との間の認証処理に大きな影響を与えることなくルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際して SSL による認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。

また、この実施形態においては、クライアント装置 40 にサーバ機能部 44 を設ける必要はあるが、ルート鍵更新処理の手順に通信要求待ちを必要とする箇所がないため、処理を速やかに進め、短期間で完了させることができる。

#### 【0129】

〔第 3 の実施形態：図 24 乃至図 27〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第 3 の実施形態の構成について説明する。

このデジタル証明書管理システムは、ルート鍵更新処理の内容が第 1 の実施形態のデジタル証明書管理システムと異なるのみであり、装置の構成は第 1 の実施形態のものと同様であるのでその説明は省略する。

#### 【0130】

このデジタル証明書管理システムにおけるルート鍵証明書の更新動作は、この発明のデ

デジタル証明書管理方法の第3の実施形態に係る動作であり、図24乃至図27のシーケンス図に示す処理を、この順で実行するものである。以下の各図に示す処理は、証明書管理装置10、サーバ装置30、クライアント装置40の各CPUが、所要の制御プログラムを実行することによって行うものである。

このデジタル証明書管理システムの証明書管理装置10は、ルート鍵証明書の更新事由を検出すると、図24のシーケンス図に示す処理を開始する。

#### 【0131】

図24に示す処理は、第1の実施形態の説明において図6に示した処理Sと対応する処理Tである。そして、まずステップS301及びS302において、図6のステップS101及びS102の場合と同様に、有効なルート私有鍵について、新たなルート私有鍵とルート鍵のペアを作成すると共に、その新ルート鍵に従前のルート私有鍵を用いたデジタル署名を付し、第1の証明鍵証明書である配布用ルート鍵証明書を作成する。

そしてさらに、ステップS303において、図11のステップS151の場合と同様に、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第2の証明鍵証明書として新ルート鍵証明書を作成する。

#### 【0132】

その後、続いて図25のシーケンス図に示す処理21を行う。この処理は、第1の実施形態の説明において図8に示した処理2及び図9に示した処理3を併せ、さらに図12に示した処理6の一部を加えた処理に相当する。

ここではまず、ステップS311で、図9のステップS131の場合と同様に、証明書管理装置10がクライアント公開鍵に新ルート私有鍵を用いたデジタル署名を付して新クライアント公開鍵証明書を作成する。

#### 【0133】

そしてステップS312で、証明書管理装置10がサーバ装置30に対して、図24のステップS302で作成した配布用ルート鍵証明書と、図24のステップS303で作成した新ルート鍵証明書と、ステップS311で作成した新クライアント公開鍵証明書と共に、これらについての更新要求をクライアント装置40に送信するよう要求する更新要求送信要求を送信する。サーバ装置30はこれに応じて、図8のステップS122及びS123の場合と同様に、クライアント装置40からの通信要求(S313)に対する応答としてこれらの証明書とそれらについての更新要求とを送信するようにしている(S314)。

以上の処理により、証明書管理装置10からクライアント装置40にサーバ装置30を介して上記の各証明書とそれらについての更新要求とが送信されることになり、ステップS312の処理においては、証明書管理装置10のCPU11が第1の送信手段として機能する。

#### 【0134】

クライアント装置40は、この要求を受け取ると、ステップS315及びS316で、図8のステップS124及びS125の場合と同様に、従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると配布用ルート鍵証明書を証明書記憶部41に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。

そしてさらにステップS317で、図12のステップS165の場合と同様に、記憶した配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップS318で新ルート鍵証明書を証明書記憶部41に記憶する。この時点で配布用ルート鍵は消去してしまってもよいが、ここでは記憶したままとする。

これらのステップS315乃至S318の処理において、クライアント装置40のCPUが第2のクライアント側更新手段として機能する。

#### 【0135】

次に、ステップS319及びS320で、図9のステップS135及びS136の場合と同様に、新クライアント公開鍵証明書の正当性を確認し、これが確認できると、新クラ

クライアント公開鍵証明書を証明書記憶部 41 に記憶する。ただし、ここでは既に新ルート鍵証明書を記憶しているため、新クライアント公開鍵証明書の正当性は、配布用ルート鍵証明書ではなく新ルート鍵証明書を用いて確認することができる。これらのステップ S 319 及び S 320 において、クライアント装置 40 の CPU が第 1 のクライアント側更新手段として機能する。

#### 【0136】

このとき、まだ従前のクライアント公開鍵証明書は消去しない。従って、証明書記憶部 41 には 2 つのクライアント公開鍵証明書が記憶された状態となる。この状態で通信相手に対して公開鍵証明書を送信する場合には、まず新公開鍵証明書を送信するものとする。ここではまだサーバ装置 30 に新ルート鍵を記憶させていないので、サーバ装置 30 は新公開鍵証明書のデジタル署名を復号化できず、認証が失敗した旨の応答を受けることになる。しかしこの場合でも、再度通信を要求し、この際に従前の公開鍵証明書を送信すれば、従前のルート鍵によってそこに付されたデジタル署名を復号化できるので、問題なく認証を受けることができる。

#### 【0137】

なお、ステップ S 319 及び S 320 の処理を、ステップ S 317 及び S 318 の処理より前に行うようにしてもよい。この場合には、ステップ S 319 における正当性の確認は、配布用ルート鍵証明書を用いて行うことになる。

クライアント装置 40 はその後、ステップ S 321 で、証明書管理装置 10 に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置 30 に対して送信し、サーバ装置 30 がステップ S 322 で証明書管理装置 10 に対して送信する。

#### 【0138】

その後、続いて図 26 のシーケンス図に示す処理 22 を行う。この処理は、第 1 の実施形態の説明において図 7 に示した処理 1 及び図 10 に示した処理 4 を併せ、さらに図 11 に示した処理 5 の一部を加えた処理に相当する。

ここではまず、ステップ S 323 で、図 10 のステップ S 141 の場合と同様に、証明書管理装置 10 がサーバ公開鍵に新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成する。

#### 【0139】

そして、ステップ S 324 で、証明書管理装置 10 がサーバ装置 30 に対して、図 24 のステップ S 302 で作成した配布用ルート鍵証明書と、図 24 のステップ S 303 で作成した新ルート鍵証明書と、ステップ S 323 で作成した新サーバ公開鍵証明書と共に、これらについての更新要求を送信する。このステップ S 324 の処理においては、証明書管理装置 10 の CPU 11 が第 2 の送信手段として機能する。

サーバ装置 30 は、この要求を受け取ると、ステップ S 325 及び S 326 で、図 7 のステップ S 112 及び S 113 の場合と同様に、従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると配布用ルート鍵証明書を証明書記憶部 31 に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。

#### 【0140】

そしてさらにステップ S 327 で、図 11 のステップ S 153 の場合と同様に、記憶した配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップ S 328 で新ルート鍵証明書を証明書記憶部 31 に記憶すると共に、配布用ルート鍵証明書と従前のルート鍵証明書を廃棄する。この時点では既にクライアント装置 40 に新クライアント公開鍵証明書を記憶させてあるので、従前のルート鍵は不要であり、改めて廃棄要求を行うよりもここで廃棄してしまった方が処理の手順が簡単になるので、このようにしたものである。もちろん、改めて廃棄要求を行うようにしてもよい。

これらのステップ S 324 乃至 S 328 において、サーバ装置 30 の CPU が第 2 のサーバ側更新手段として機能する。

#### 【0141】

次に、ステップ S 3 2 9 及び S 3 3 0 で、図 1 0 のステップ S 1 4 3 及び S 1 4 4 の場合と同様に、新サーバ公開鍵証明書の正当性を確認し、これが確認できると、新サーバ公開鍵証明書を証明書記憶部 3 1 に記憶し、従前のサーバ公開鍵証明書と置き換える。ただし、ここでは既に新ルート鍵証明書を記憶しているので、新クライアント公開鍵証明書の正当性は、配布用ルート鍵証明書ではなく新ルート鍵証明書を用いて確認することができる。これらのステップ S 3 2 9 及び S 3 3 0 において、サーバ装置 3 0 の CPU が第 1 のサーバ側更新手段として機能する。

#### 【0142】

このとき従前のサーバ公開鍵証明書を消去する理由は、第 1 の実施形態において図 9 の説明で述べた通りである。そして、ステップ S 3 3 0 の時点では既にクライアント装置に新ルート鍵を記憶させてあるので、新サーバ公開鍵証明書を記憶させておけば、認証処理には全く問題ない。

なお、ステップ S 3 2 9 及び S 3 3 0 の処理を、ステップ S 3 2 7 及び S 3 2 8 の処理より前に行うようにしてもよい。この場合には、ステップ S 3 2 9 における正当性の確認は、配布用ルート鍵証明書を用いて行うことになる。

#### 【0143】

サーバ装置 3 0 はその後、ステップ S 3 3 1 で証明書管理装置 1 0 に対して更新要求に対する応答として結果通知を返す。

以上の図 2 6 に示す処理により、サーバ装置 3 0 側ではルート鍵更新処理が完了する。

#### 【0144】

その後、続いて図 2 7 のシーケンス図に示す処理 2 3 を行う。

ここではまずステップ S 3 3 2 で、証明書管理装置 1 0 がサーバ装置 3 0 に対して、不要になったデジタル証明書の廃棄を求める旧鍵廃棄要求をクライアント装置 4 0 に送信するよう要求する旧鍵廃棄要求送信要求を送信する。サーバ装置 3 0 は、これに応じて、クライアント装置 4 0 からの通信要求 (S 3 3 3) に対する応答として旧鍵廃棄要求を送信するようにしている (S 3 3 4)。

以上の処理により、証明書管理装置 1 0 からクライアント装置 4 0 にサーバ装置 3 0 を介して上記の旧鍵廃棄要求が送信されることになる。

#### 【0145】

クライアント装置 4 0 は、この要求を受け取ると、ステップ S 3 3 5 で、証明書記憶部 4 1 に記憶している配布用ルート鍵証明書、従前のルート鍵証明書、および従前のクライアント公開鍵証明書を廃棄する。この時点では、サーバ装置 3 0 に新ルート鍵証明書及び新サーバ公開鍵証明書が記憶されているので、これらの証明書を消去しても認証処理に影響はない。

クライアント装置 4 0 はその後、ステップ S 3 3 6 で証明書管理装置 1 0 に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置 3 0 に対して送信し、サーバ装置 3 0 がステップ S 3 3 7 で証明書管理装置 1 0 に対して送信する。

以上により、ルート鍵更新処理を終了する。

#### 【0146】

このデジタル証明書管理システムにおいても、ルート鍵更新処理をこのような手順で行うことにより、第 1 の実施形態の場合と同様に、サーバ装置 3 0 とクライアント装置 4 0 との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際して SSL による認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。

#### 【0147】

なお、この実施形態では、サーバ装置 3 0 に新ルート鍵を記憶させる前にクライアント装置 4 0 に新クライアント公開鍵証明書を記憶させるので、サーバ装置 3 0 に新ルート鍵を記憶させるまでは、通信に、新クライアント公開鍵証明書のデジタル署名をサーバ装置

30が復号化できないことによるオーバーヘッドが生じる。しかし一方で、証明書管理装置10からサーバ装置30（あるいはサーバ装置30を介してクライアント装置40）に計3回の要求を送信するのみでルート鍵の更新処理を行うことができる。従って、6回の要求送信が必要な第1の実施形態の場合と比較して、処理手順の管理やプログラムの設計が容易であるという効果がある。ルート鍵証明書を更新すべきサーバ装置やクライアント装置の数が多い場合には、この効果はより大きくなり、この実施形態が有効である。

また、処理21や処理22において、各証明書について正当性を確認した後で必要なものを一括して記憶するようにすれば、証明書を記憶する不揮発メモリへのアクセス回数を低減し、処理負荷を低減すると共に処理を高速化することができる。

#### 【0148】

〔第4の実施形態：図24，図28乃至図30〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第4の実施形態の構成について説明する。

このデジタル証明書管理システムは、ルート鍵更新処理の内容が第2の実施形態のデジタル証明書管理システムと異なるのみであり、装置の構成は第2の実施形態のものと同様であるのでその説明は省略する。

#### 【0149】

このデジタル証明書管理システムにおけるルート鍵証明書の更新動作は、この発明のデジタル証明書管理方法の第4の実施形態に係る動作であり、図24及び図28乃至図30のシーケンス図に示す処理T及び処理31乃至33を、この順で実行するものである。以下の各図に示す処理は、証明書管理装置10，サーバ装置30，クライアント装置40の各CPUが、所要の制御プログラムを実行することによって行うものである。

#### 【0150】

また、これらの処理は、図24に示す部分については第3の実施形態の場合と共通であり、図28乃至図30に示す部分については、第3の実施形態で図25乃至図27を用いてそれぞれ説明した処理と同じ目的の処理であり、証明書管理装置10と直接通信する装置がクライアント装置40であることに伴って、第2の実施形態で図17及び図18を用いて説明した処理11及び処理12の場合と同様に通信手順を若干変更したのみである。そこで、これらの処理についての詳細な説明は省略する。

#### 【0151】

そして、この第4の実施形態のデジタル証明書管理システムにおいても、ルート鍵更新処理をこのような手順で行うことにより、証明書管理装置10がクライアント・サーバシステムを構成する装置のうちクライアント装置40のみと通信可能な場合でも、第3の実施形態の場合と同様に、サーバ装置30とクライアント装置40との間の認証処理に大きな影響を与えることなくルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してSSLによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。また、処理手順の管理やプログラムの設計が容易であるという効果もある。

#### 【0152】

〔変形例〕

以上説明した実施形態では、クライアント装置40とサーバ装置30とが図4や図5を用いて説明したようなSSLによる認証処理を行う場合の例について説明した。しかし、この認証処理が必ずしもこのようなものでなくてもこの発明は効果を発揮する。

SSLを改良したTLS (Transport Layer Security) も知られているが、このプロトコルに基づく認証処理を行う場合にも当然適用可能である。

#### 【0153】

また、上述した実施形態では、証明書管理装置10をサーバ装置30あるいはクライアント装置40とは別に設ける例について説明したが、サーバ装置30あるいはクライアン

ト装置 40 と一体として設けることを妨げるものではない。この場合、証明書管理装置 10 の機能を実現するための CPU, ROM, RAM 等の部品を独立して設けてもよいが、ハードウェア資源としてはサーバ装置 30 あるいはクライアント装置 40 の CPU, ROM, RAM 等を使用し、その CPU に適当なソフトウェアを実行させることにより、証明書管理装置 10 として機能させるようにしてもよい。

#### 【0154】

このような場合において、証明書管理装置 10 と、これと一体になっているサーバ装置 30 あるいはクライアント装置 40 との間の通信には、ハードウェアを証明書管理装置 10 として機能させるためのプロセスと、ハードウェアをサーバ装置 30 あるいはクライアント装置 40 として機能させるためのプロセスとの間のプロセス間通信を含むものとする。

さらに、上述した各実施形態では、証明書管理装置 10 が証明鍵やデジタル証明書を自ら作成してこれを取得する例について説明したが、図 2 及び図 16 に示した証明用鍵作成部 21 や証明書発行部 22 の機能を証明書管理装置 10 とは別の装置に設け、証明書管理装置 10 がその装置から証明鍵やデジタル証明書の供給を受けてこれらを取得するようにしてもよい。

#### 【0155】

また、証明書管理装置 10 がサーバ装置 30 及びクライアント装置 40 の双方と直接的に通信が可能な構成としても構わない。この場合、図 7 乃至図 12 等 に示した通信シーケンスは、双方の装置と直接通信が可能であることに伴って異なったものになるが、処理の順序は上述した各実施形態の場合と同様である。このようにしても、上述した各実施形態の効果をを得ることができる。

#### 【0156】

また、上述したように、第 2 及び第 4 の実施形態においては、証明書管理装置 10 とクライアント装置 40 との間で通信を行う際にも、SSL による認証処理を行うようにすることができる。

このようにするには、図 31 に示すように、クライアント装置 40 に、サーバ装置 30 との間の認証処理に用いるクライアント私有鍵、クライアント公開鍵証明書及びルート鍵証明書（実施形態において説明したもの）とは別に、もう一組の私有鍵、公開鍵証明書及びルート鍵証明書（「第 2 のクライアント私有鍵」、「第 2 のクライアント公開鍵証明書」及び「第 2 のルート鍵証明書」と呼ぶ）を記憶させ、証明書管理装置 10 との間の認証処理にこれらを用いるようにすればよい。

#### 【0157】

この場合、証明書管理装置 10 にも、管理装置用私有鍵、管理装置用公開鍵証明書及び上記の第 2 のルート鍵証明書を記憶させ、認証処理に用いる。そして、第 2 のクライアント公開鍵証明書及び管理装置用公開鍵証明書は、第 2 のルート鍵証明書に含まれる第 2 のルート鍵で内容が確認できるものとする。すなわち、その第 2 のルート鍵と対応するルート私有鍵（第 2 のルート私有鍵）を用いてデジタル署名を付すようにする。

このようにすれば、証明書管理装置 10 とクライアント装置 40 との間の認証処理と、クライアント装置 40 とサーバ装置 30 との間の認証処理とを、全く独立して行うことができる。

#### 【0158】

第 2 及び第 4 の実施形態におけるクライアント装置 40 は、図 16 を用いて説明したように、証明書管理装置 10 との通信はサーバ機能部 44 が、サーバ装置 30 との通信はクライアント機能部 43 が通信機能部 42 を介して行う。従って、証明書管理装置 10 から通信を要求される通信と、サーバ装置 30 に要求する通信とは明確に区別することができるため、これらとの間で別々の鍵や証明書を用いた認証処理を行うことができるのである。

このような場合において、証明書管理装置 10 からの要求に応じてクライアント装置 40 とサーバ装置 30 との間の認証処理に用いるルート鍵証明書や公開鍵証明書を更新した

としても、証明書管理装置 10 とクライアント装置 40 との間の認証処理には全く影響がない。

#### 【0159】

各実施形態で説明した手順によって更新処理を行えば、クライアント装置 40 とサーバ装置 30 との間の認証処理にも大きな影響を与えることなく更新処理を行えることは上述した通りであるので、図 31 に示した構成をとることにより、各ノード間の認証処理を維持したままルート鍵を更新できると言える。

なお、第 2 のルート鍵証明書を更新しようとする場合には、証明書管理装置 10 をクライアント、クライアント装置 40 をサーバとして、上述したいずれかの実施形態の手順に従って更新処理を行えばよい。このような更新処理を行っても、クライアント装置 40 とサーバ装置 30 との間の認証処理には全く影響がない。

#### 【0160】

また、上述した各実施形態においては、クライアント装置 40 とサーバ装置 30 とが相互認証を行う際に必要な、クライアント装置 40 とサーバ装置 30 の双方に記憶させているルート鍵証明書及び公開鍵証明書を更新する例について説明した。しかし、図 5 を用いて説明したように、クライアント装置 40 がサーバ装置 30 を認証するのみでよいのであれば、クライアント装置 40 に公開鍵証明書を、サーバ装置 30 にルート鍵証明書を記憶させておけば足りる。従って、更新についてもこれらのみを更新すれば足りる。

そこで、例えば第 1 の実施形態に示したルート鍵証明書の更新処理を、以下のように簡略化することができる。すなわち、図 34 に示すように、図 6 に示したルート鍵証明書作成処理（処理 S）、図 8 に示したクライアント装置のルート鍵証明書記憶処理（処理 2）、図 32 に示すサーバ装置の公開鍵証明書記憶処理（処理 24）、図 33 に示すクライアント装置のルート鍵証明書書き換え処理（処理 26）を、この順番で実行するようにすればよい。

#### 【0161】

これらの処理において、処理 24 は、図 10 に示した処理 4 と対応するものであるが、サーバ装置 30 にルート鍵証明書を記憶させない場合には、ステップ S144 では、証明書管理装置 10 から受信した新サーバ公開鍵証明書を信用し、そのまま従前のサーバ公開鍵証明書を置き換えるようにしている。また、ステップ S142' で配布用ルート鍵証明書も送信し、これを用いて新サーバ公開鍵証明書の正当性を確認できるようにしてもよい（S143）。このようにする場合、サーバ装置 30 側にもクライアント装置 40 側と同じルート鍵証明書を記憶しておくようにすれば、これを用いて配布用ルート鍵証明書の正当性を確認することもできる。

また、処理 26 は、図 12 に示した処理 6 と対応するものであり、クライアント装置 40 側には公開鍵証明書を更新しないことから、ステップ S166' から公開鍵証明書を廃棄する処理を除いた点が、処理 6 と異なるのみである。

#### 【0162】

以上のような処理においても、サーバ装置 30 に対して新サーバ公開鍵証明書を送信する動作を、クライアント装置 40 から新ルート鍵証明書を受信した旨の情報を受信した後に行うことに変わりはない。そして、このようにすることにより、第 1 の実施形態の場合と同様に、サーバ装置 30 とクライアント装置 40 との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。

なお、第 2 乃至第 4 の実施形態についても同様にこのような変形を適用可能であることは、いうまでもない。

#### 【0163】

また、上述した各実施形態においては、クライアント装置 40 とサーバ装置 30 で共通のルート鍵証明書を用いる例について説明したが、必ずしもこのようにする必要はない。すなわち、図 35 に示すように、クライアント装置 40 とサーバ装置 30 で別々のルート鍵証明書を記憶させるようにしてもよい。このようにしても、サーバ装置 30 側でクライアント公開鍵証明書の正当性を確認でき、クライアント装置 40 側でサーバ公開鍵証明書



の正当性を確認できれば、認証処理には全く問題ない。

#### 【0164】

そして、このような場合には、各ルート鍵証明書を独立して更新することが考えられ、その場合にはそのルート鍵証明書を用いて正当性を確認すべき公開鍵証明書も共に更新することになる。そして、このような処理も、上述した各実施形態の場合と同様な考え方により、クライアント装置40側に記憶させているルート鍵証明書（サーバルート鍵証明書）の更新が終了した後でサーバ装置30側に記憶させている公開鍵証明書（サーバ公開鍵証明書）を更新するようにすれば、クライアント装置40とサーバ装置30との間の認証処理が可能な状態のまま、ルート鍵を更新することができる。サーバ装置30側に記憶させているルート鍵証明書（クライアントルート鍵証明書）の更新が終了した後でクライアント装置40側に記憶させている公開鍵証明書（クライアント公開鍵証明書）を更新するようにするとよいことも、第1の実施形態で説明した場合と同様である。

#### 【0165】

この処理の具体例を示すと、例えば、図36乃至図39に示す各処理を、図40に示す順番で実行すればよい。図36乃至図39に示す各処理は、それぞれ第1の実施形態で図6に示した処理S、図8に示した処理2、図10に示した処理4、図12に示した処理6に対応するものである。

そして、図36のステップS503にて作成した確認用ルート鍵証明書は、サーバ装置30に新サーバ公開鍵証明書の正当性を確認させるために使用するものである。ここでは、サーバ公開鍵証明書はクライアント用ルート鍵証明書を用いて正当性を確認するものであり、サーバ装置30は、自身で記憶しているサーバ用ルート鍵証明書ではサーバ公開鍵証明書の正当性を確認できないため、確認用ルート鍵証明書が必要になっている。

なお、このような変形も、第2乃至第4の実施形態に同様に適用可能であることは、いうまでもない。

また、上述の各実施形態及び変形例で説明した技術を相互に組み合わせて用いることも当然可能である。

#### 【0166】

また、この発明によるプログラムは、クライアント・サーバシステムを構成する複数の装置とネットワークを介して直接的又は間接的に通信可能なコンピュータに、各機能（証明鍵更新手段、第1の送信手段、第2の送信手段、その他の手段としての機能）を実現させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

#### 【0167】

このようなプログラムは、はじめからコンピュータに備えるROMあるいはHDD等の記憶手段に格納しておいてもよいが、記録媒体であるCD-ROMあるいはフレキシブルディスク、SRAM、EEPROM、メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてCPUに実行させるか、CPUにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

#### 【産業上の利用可能性】

#### 【0168】

以上説明してきた通り、この発明のデジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法、またはプログラムによれば、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることができる。

従って、この発明を、クライアント・サーバシステムにおいて認証処理に使用する証明書の管理に適用することにより、安全に認証用公開鍵の更新が可能なシステムを安価に提

供することができる。

【図面の簡単な説明】

【0169】

【図1】この発明のデジタル証明書管理装置の実施形態である証明書管理装置のハードウェア構成を示すブロック図である。

【図2】この発明のデジタル証明書管理システムの第1の実施形態を構成する各装置の、その特徴となる部分の機能構成を示す機能ブロック図である。

【図3】図2に示したデジタル証明書管理システムにおけるデータ送受モデルを示す概念図である。

【図4】クライアント装置とサーバ装置とがSSLによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図5】クライアント装置とサーバ装置とがSSLによる片方向認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図6】図2に示したデジタル証明書管理システムにおけるルート鍵更新処理のうち、ルート鍵証明書作成処理を示すシーケンス図である。

【図7】同じくサーバ装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図8】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図9】同じくクライアント装置の公開鍵証明書記憶処理を示すシーケンス図である。

【図10】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。

【0170】

【図11】同じくサーバ装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図12】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図13】第1の実施形態のルート鍵更新処理における、図6乃至図12のシーケンス図に示した各処理の実行順を示すフローチャートである。

【図14】図7に示したシーケンスの変形例を示す図である。

【図15】図8に示したシーケンスの変形例を示す図である。

【図16】この発明のデジタル証明書管理システムの第2の実施形態を構成する各装置の、その特徴となる部分の機能構成を示す機能ブロック図である。

【図17】図16に示したデジタル証明書管理システムにおけるルート鍵更新処理のうち、サーバ装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図18】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図19】同じくクライアント装置の公開鍵証明書記憶処理を示すシーケンス図である。

【図20】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。

【0171】

【図21】同じくサーバ装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図22】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図23】第2の実施形態のルート鍵更新処理における、図6及び図17乃至図22のシーケンス図に示した各処理の実行順を示すフローチャートである。

【図24】この発明のデジタル証明書管理システムの第3の実施形態におけるルート鍵更新処理の一部を示すシーケンス図である。

- 【図 25】図 24 の続きの処理を示すシーケンス図である。  
【図 26】図 25 の続きの処理を示すシーケンス図である。  
【図 27】図 26 の続きの処理を示すシーケンス図である。  
【図 28】この発明のデジタル証明書管理システムの第 4 の実施形態におけるルート鍵更新処理の、図 24 の続きの処理を示すシーケンス図である。  
【図 29】図 28 の続きの処理を示すシーケンス図である。  
【図 30】図 29 の続きの処理を示すシーケンス図である。

【0172】

- 【図 31】この発明のデジタル証明書管理システムの各実施形態の変形例における鍵及び証明書の記憶状態及びその場合のルート鍵更新処理について説明するための図である。  
【図 32】各実施形態の変形例におけるサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。  
【図 33】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。  
【図 34】同じく各処理の実行順を示すフローチャートである。  
【図 35】各実施形態の別の変形例における、鍵及び証明書の記憶状態及びその場合のルート鍵更新処理について説明するための図である。  
【図 36】その別の変形例におけるルート鍵証明書作成処理を示すシーケンス図である。  
【図 37】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。  
【図 38】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。  
【図 39】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。  
【図 40】同じく各処理の実行順を示すフローチャートである。  
【図 41】公開鍵暗号を用いた認証処理におけるルート鍵、ルート私有鍵、およびサーバ公開鍵の関係について説明するための図である。

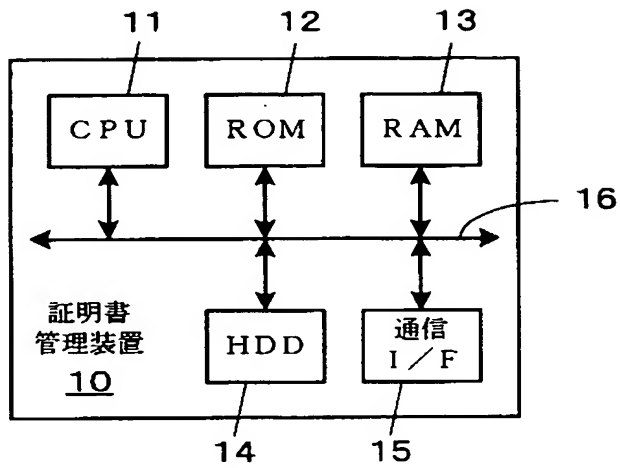
【符号の説明】

【0173】

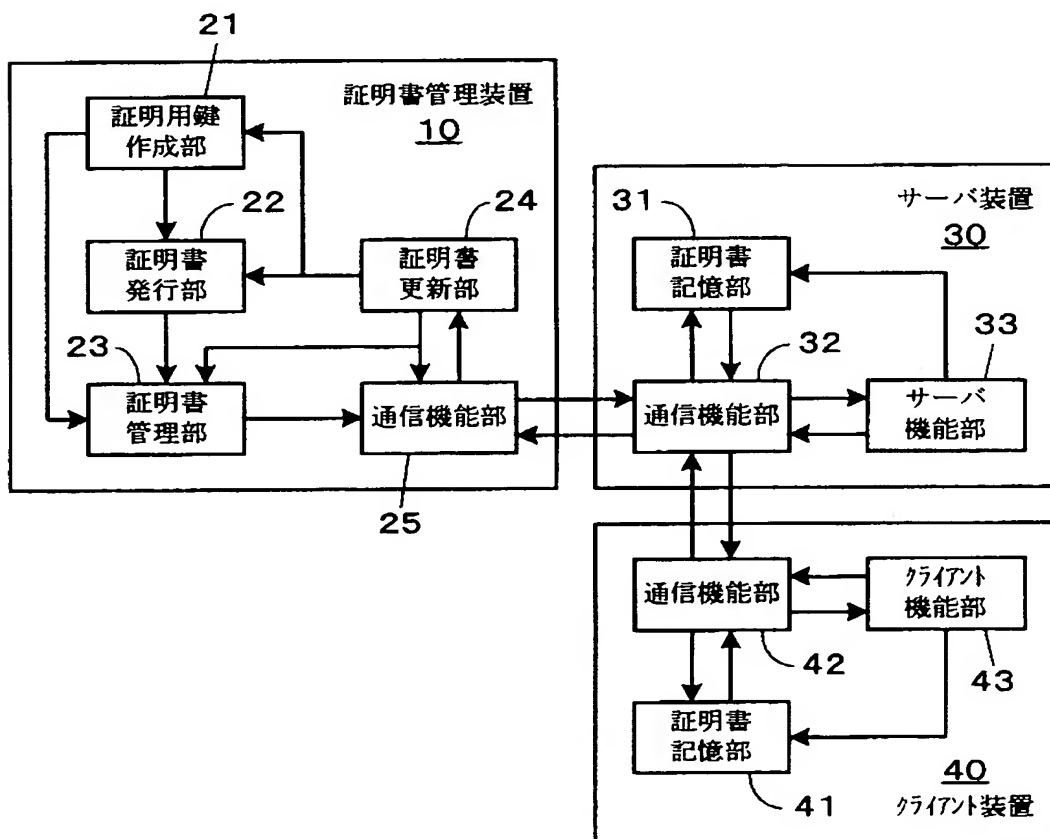
10: 証明書管理装置	11: CPU
12: ROM	13: RAM
14: HDD	15: 通信 I/F
16: システムバス	21: 証明用鍵作成部
22: 証明書発行部	23: 証明書管理部
24: 証明書更新部	25, 32, 42: 通信機能部
30: サーバ装置	31, 41: 証明書記憶部
33, 44: サーバ機能部	40: クライアント装置
43: クライアント機能部	

【書類名】 図面

【図 1】

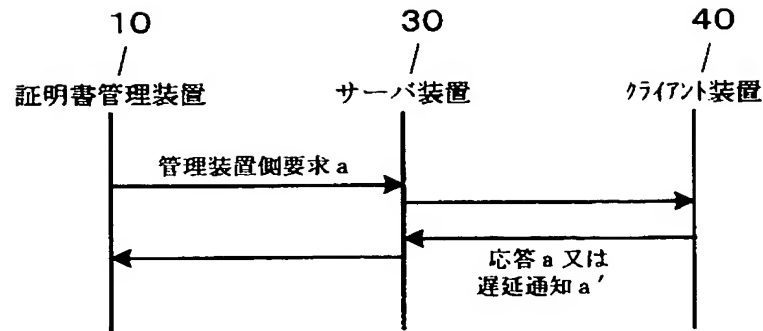


【図 2】

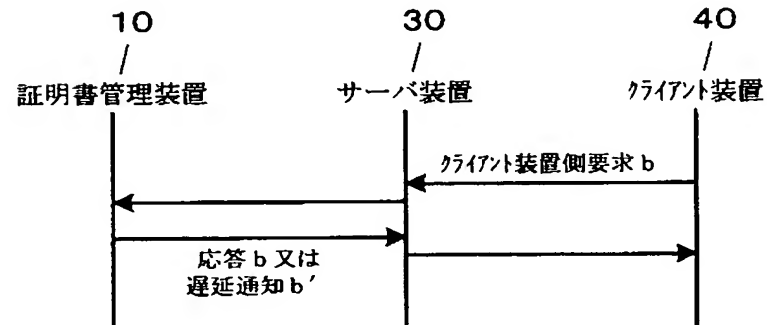


【図 3】

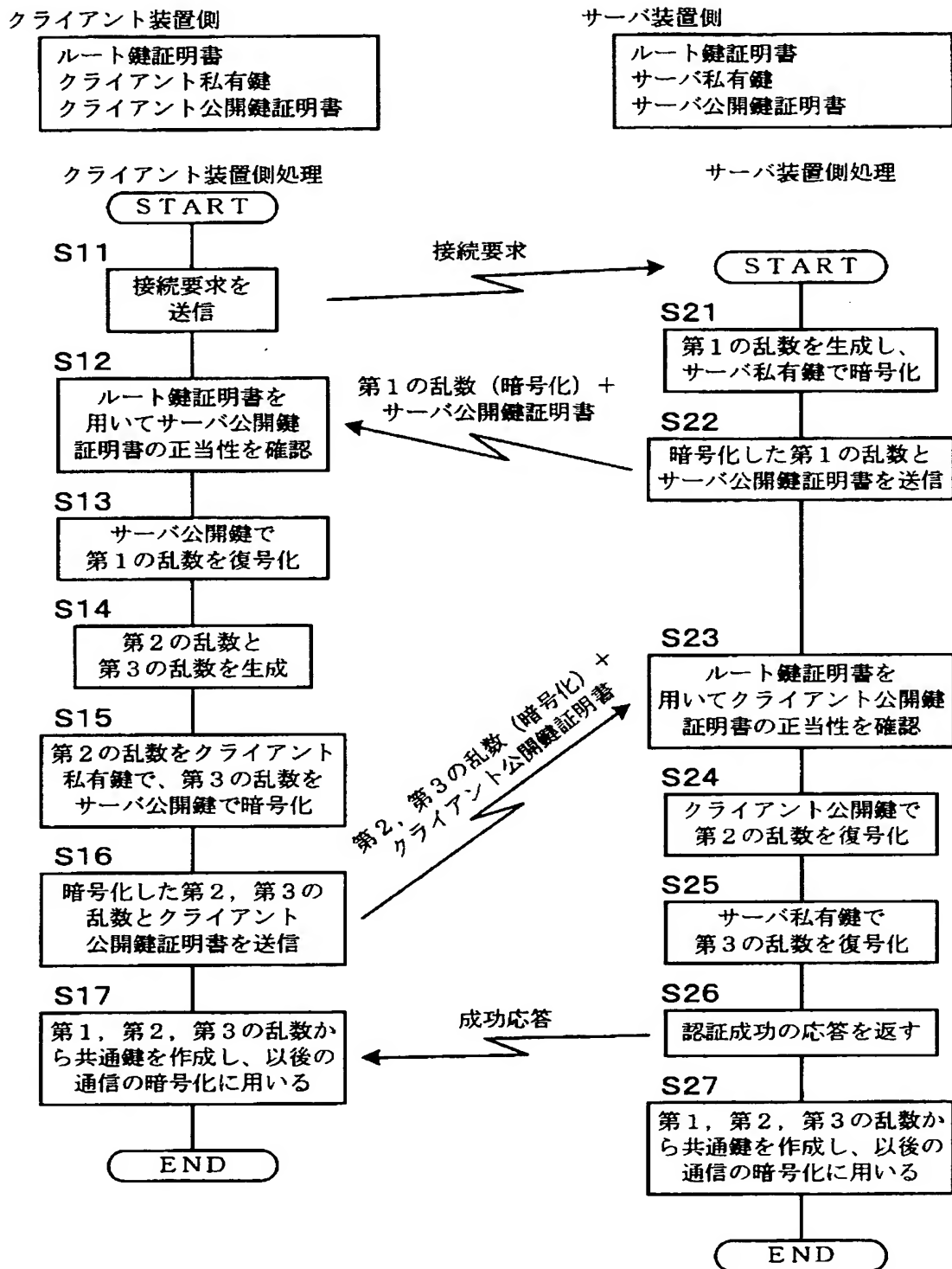
(A)



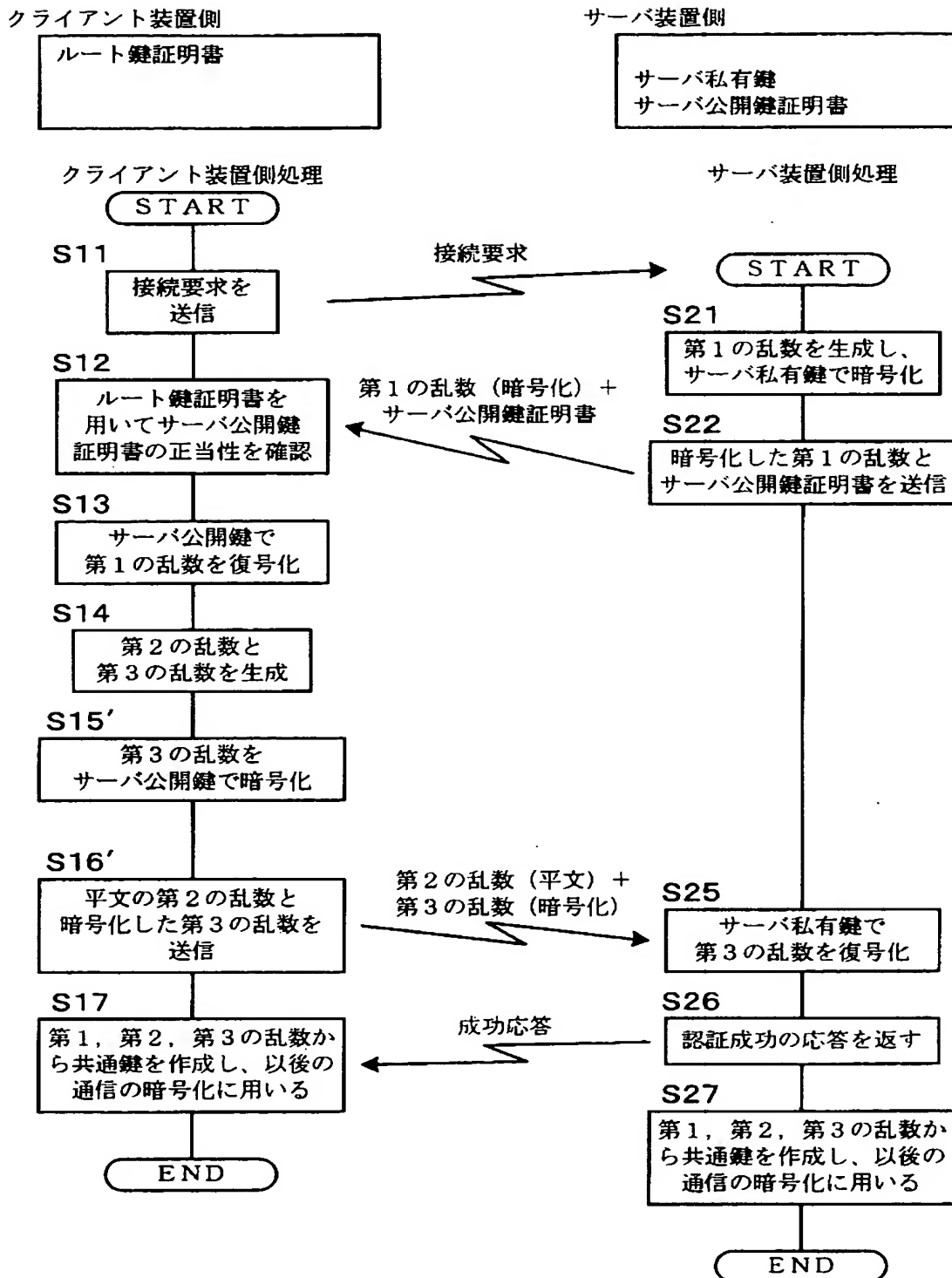
(B)



【図 4】

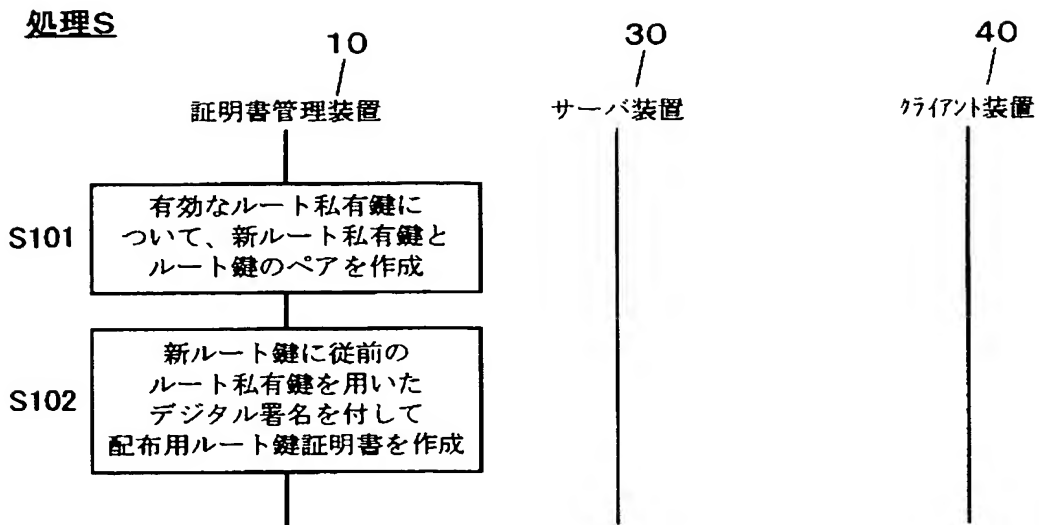


【図 5】

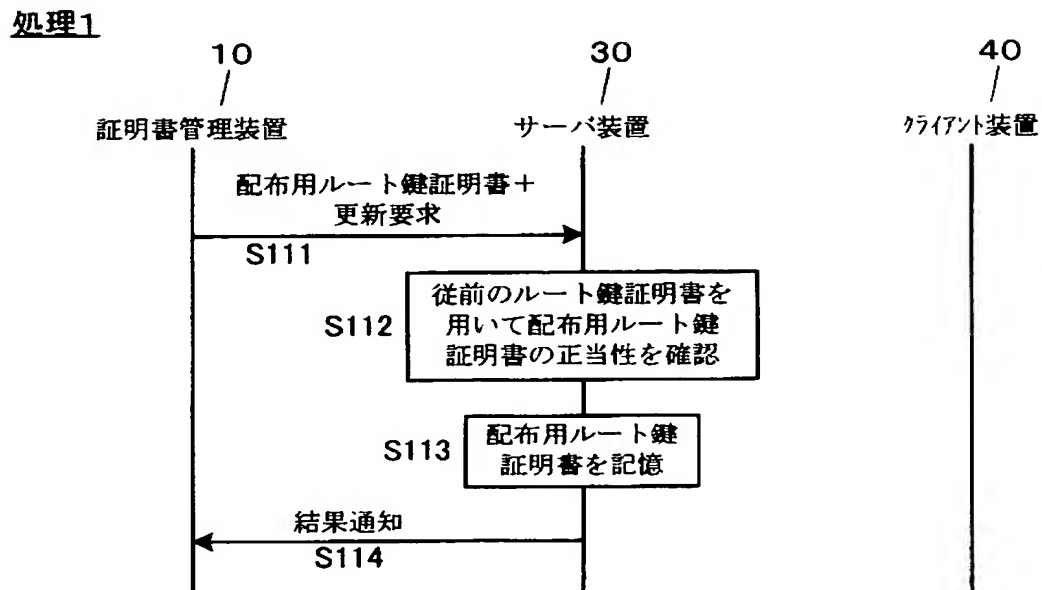




【図 6】

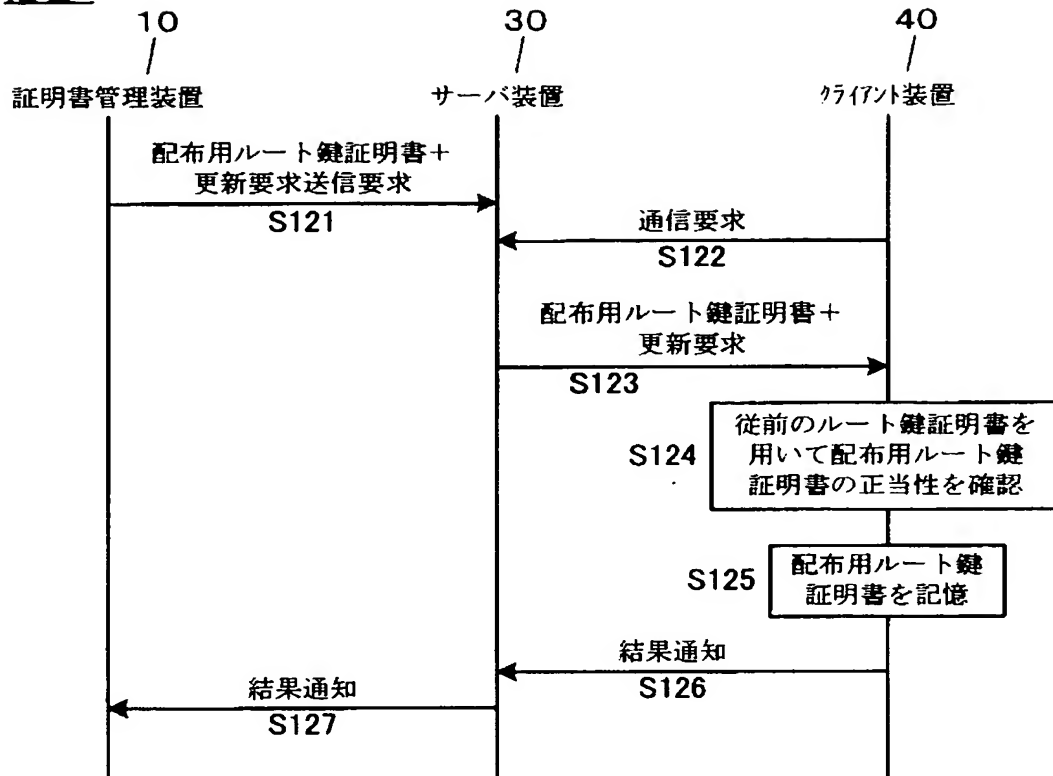


【図 7】

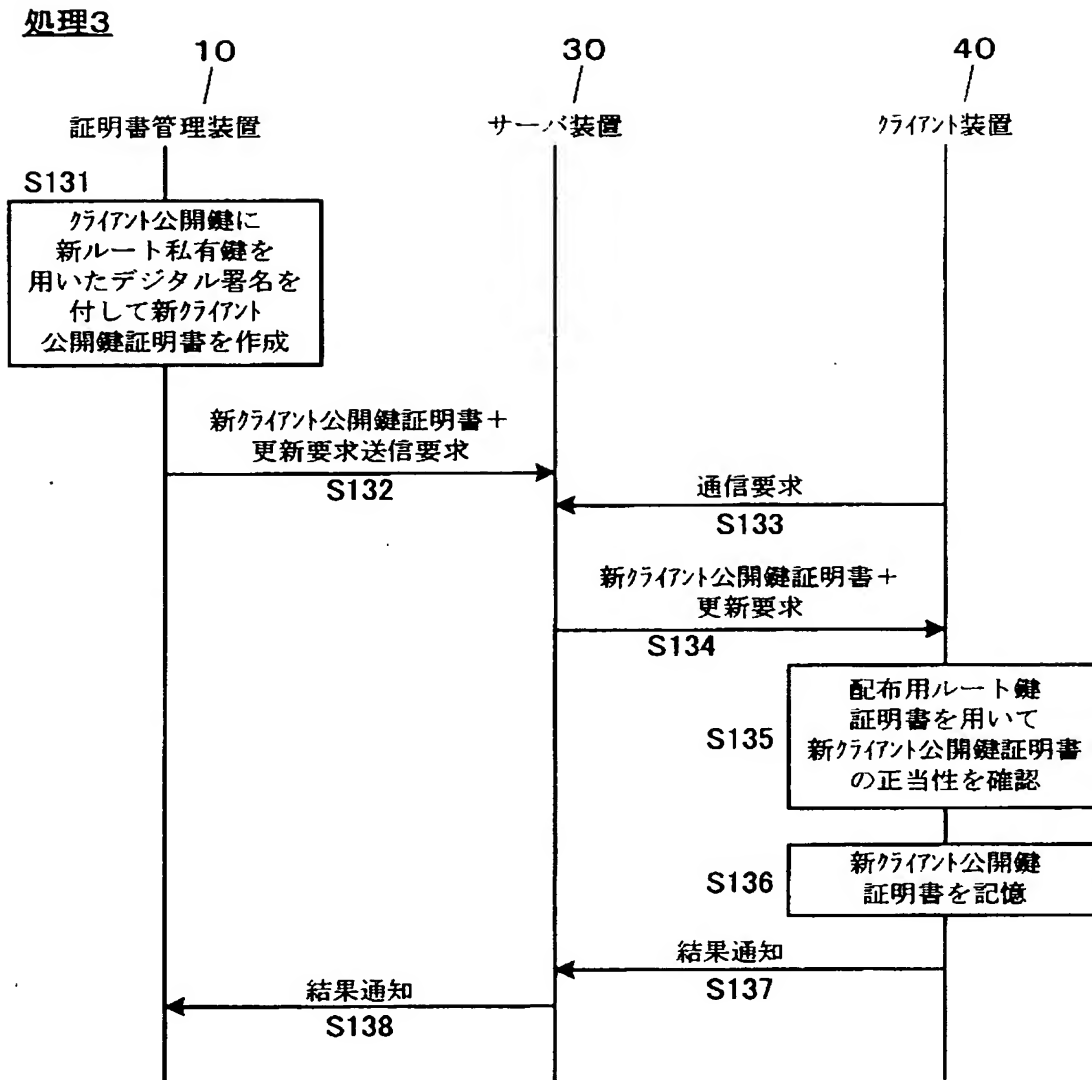


【図 8】

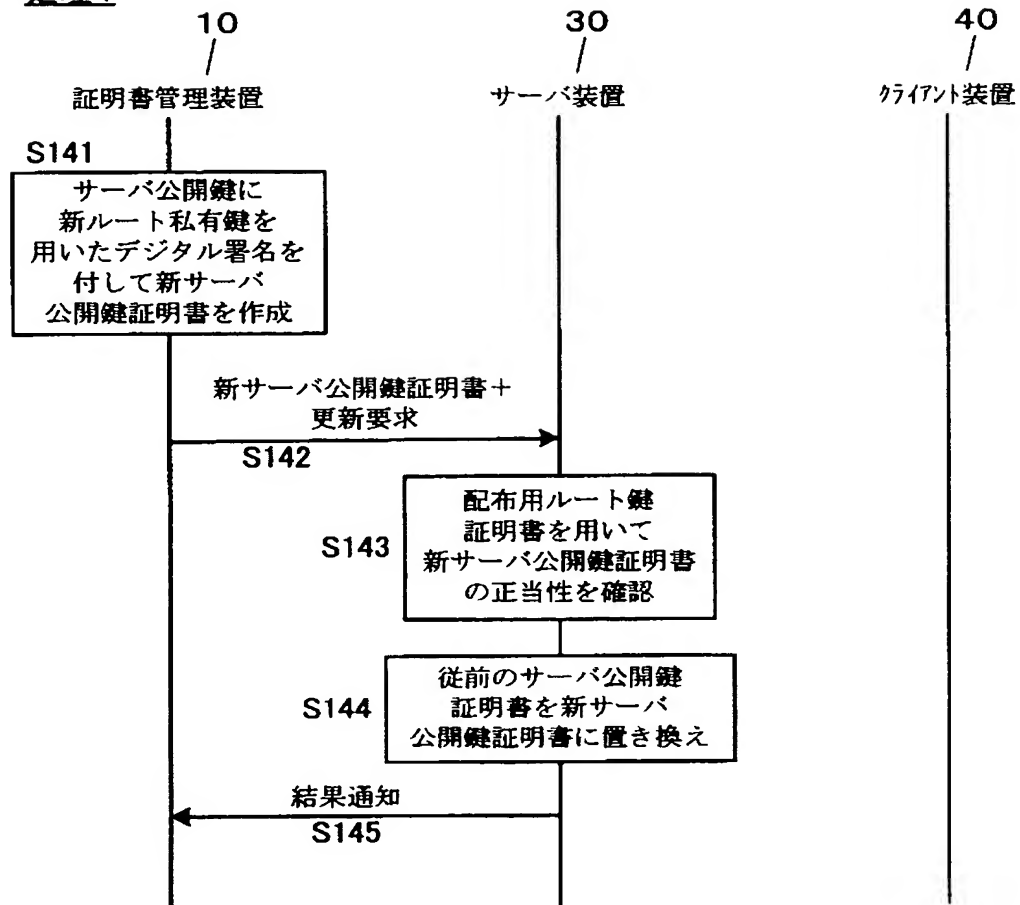
## 処理2



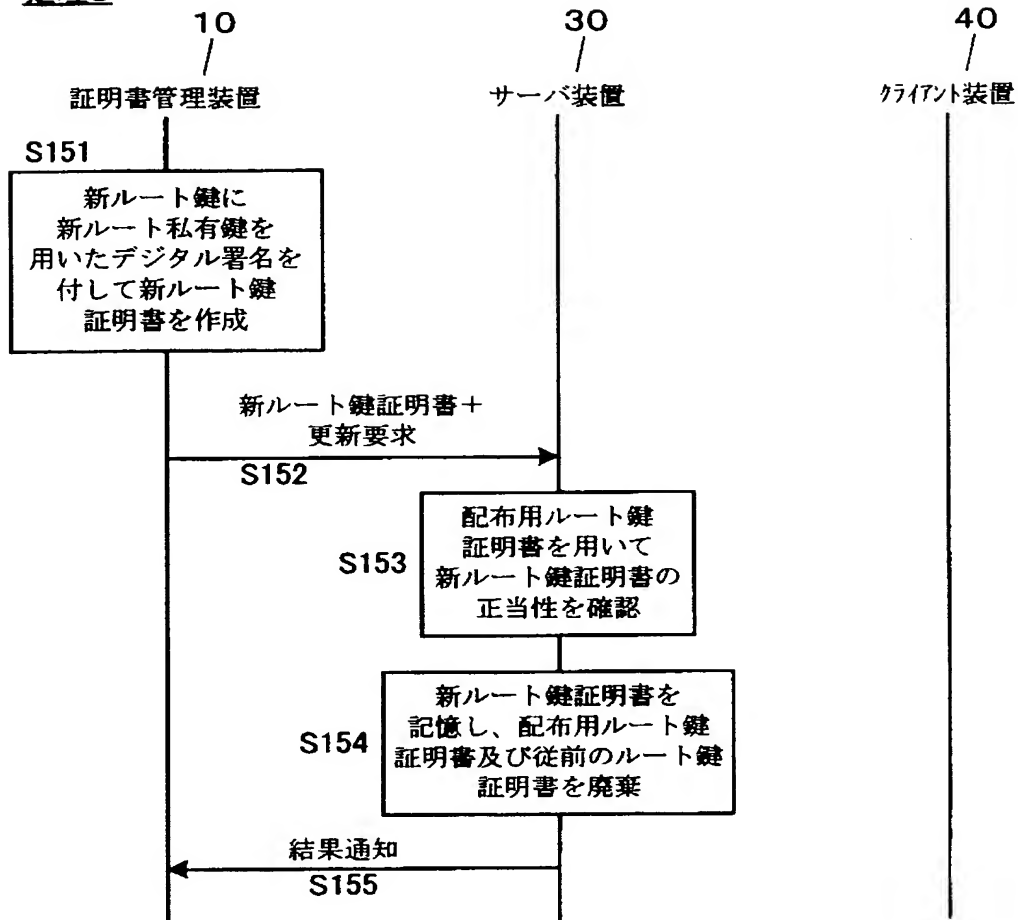
【図 9】



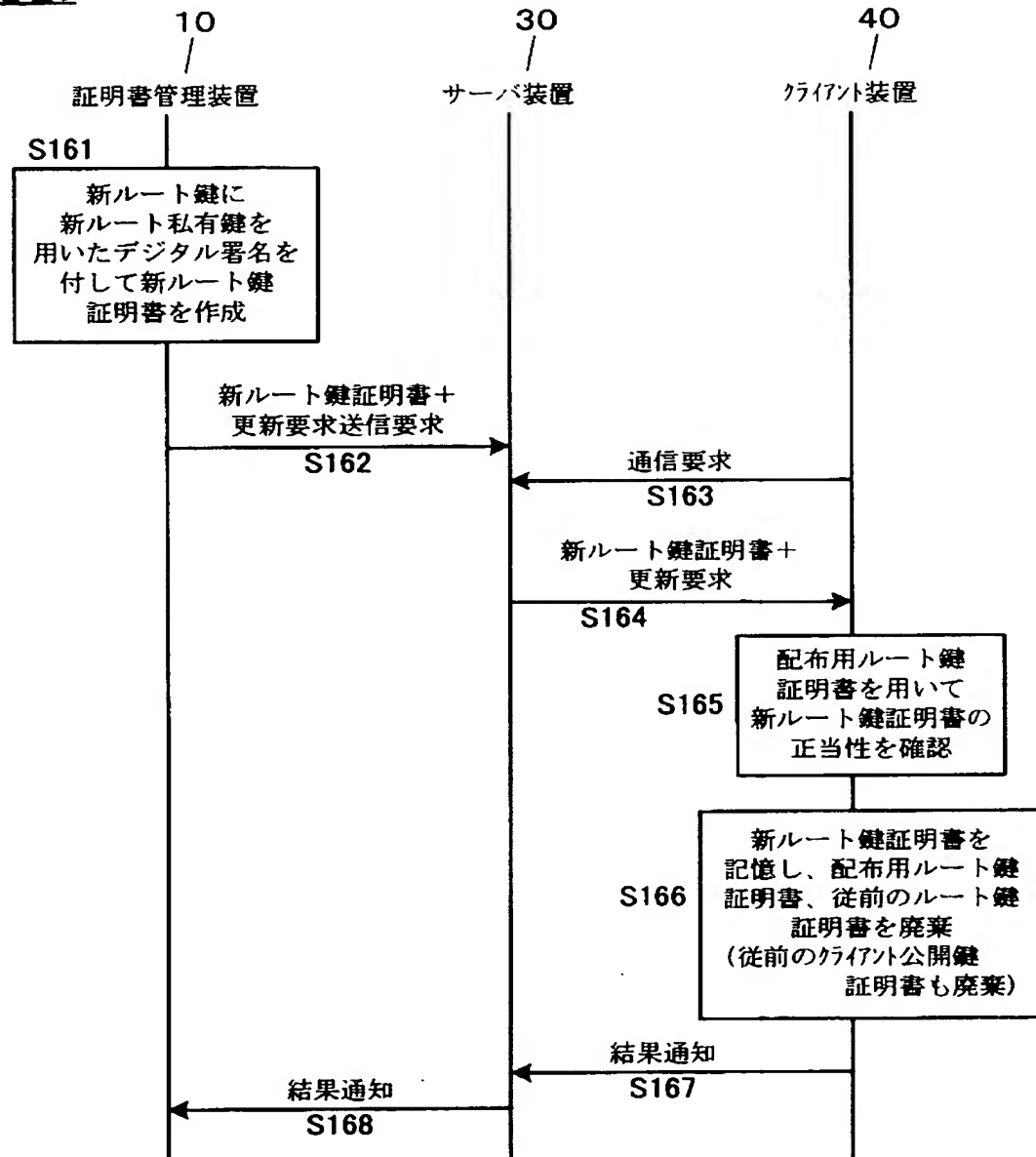
【図10】

処理4

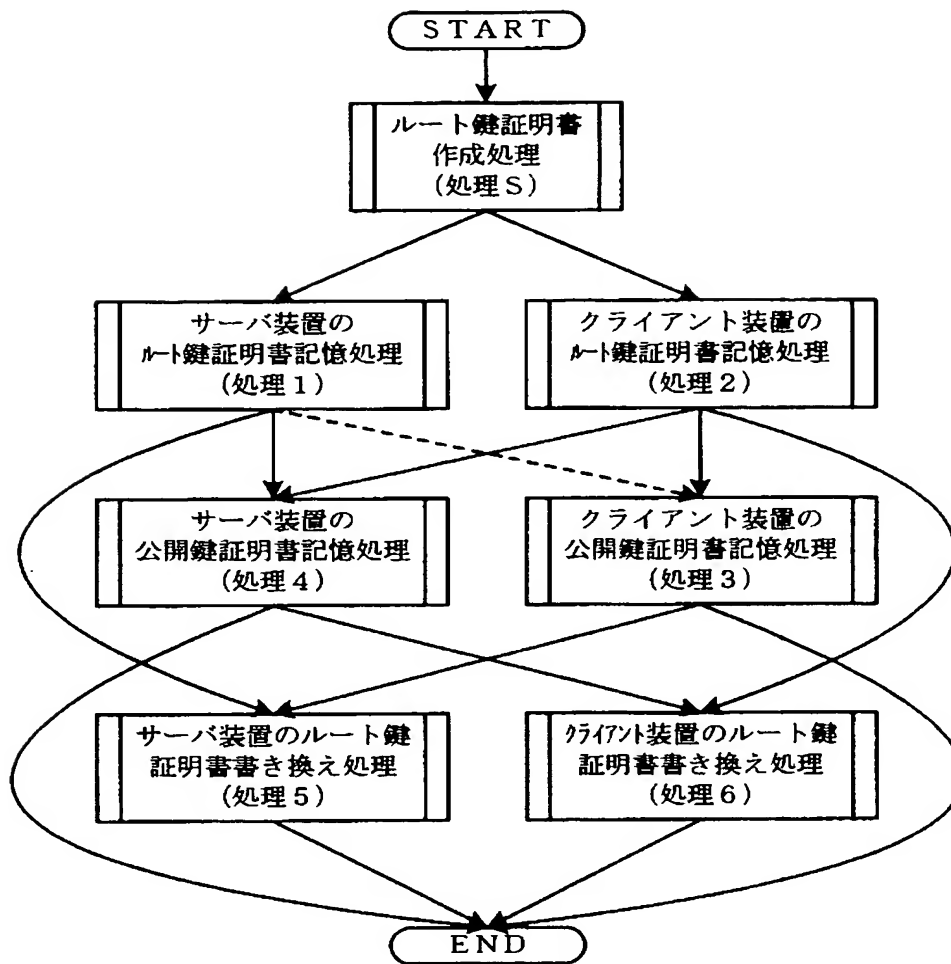
【図 11】

処理5

【図 12】

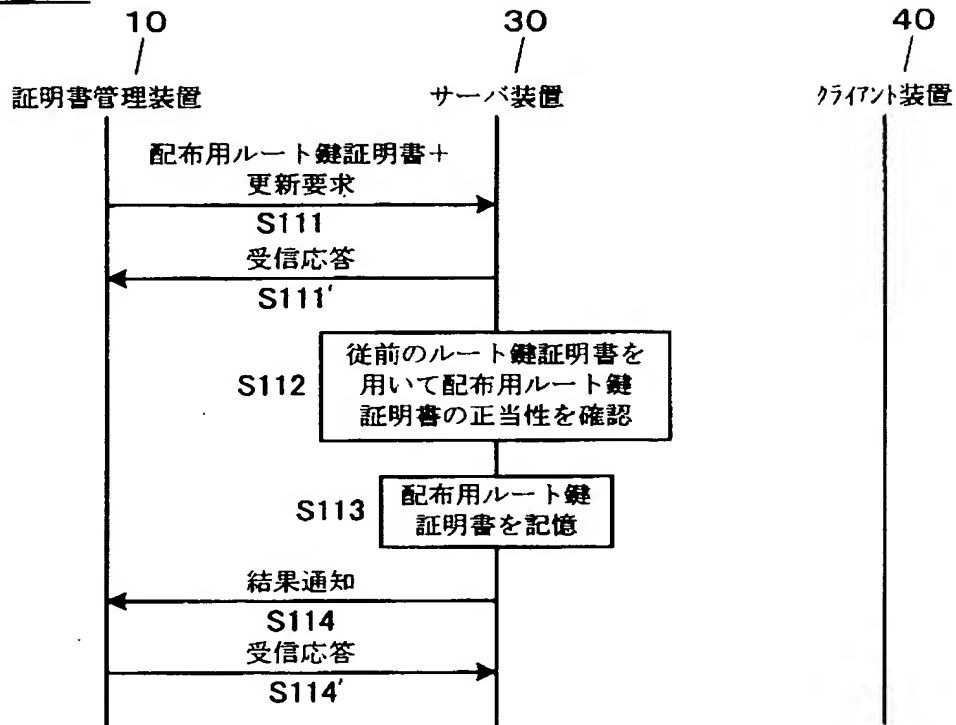
処理6

【図 13】



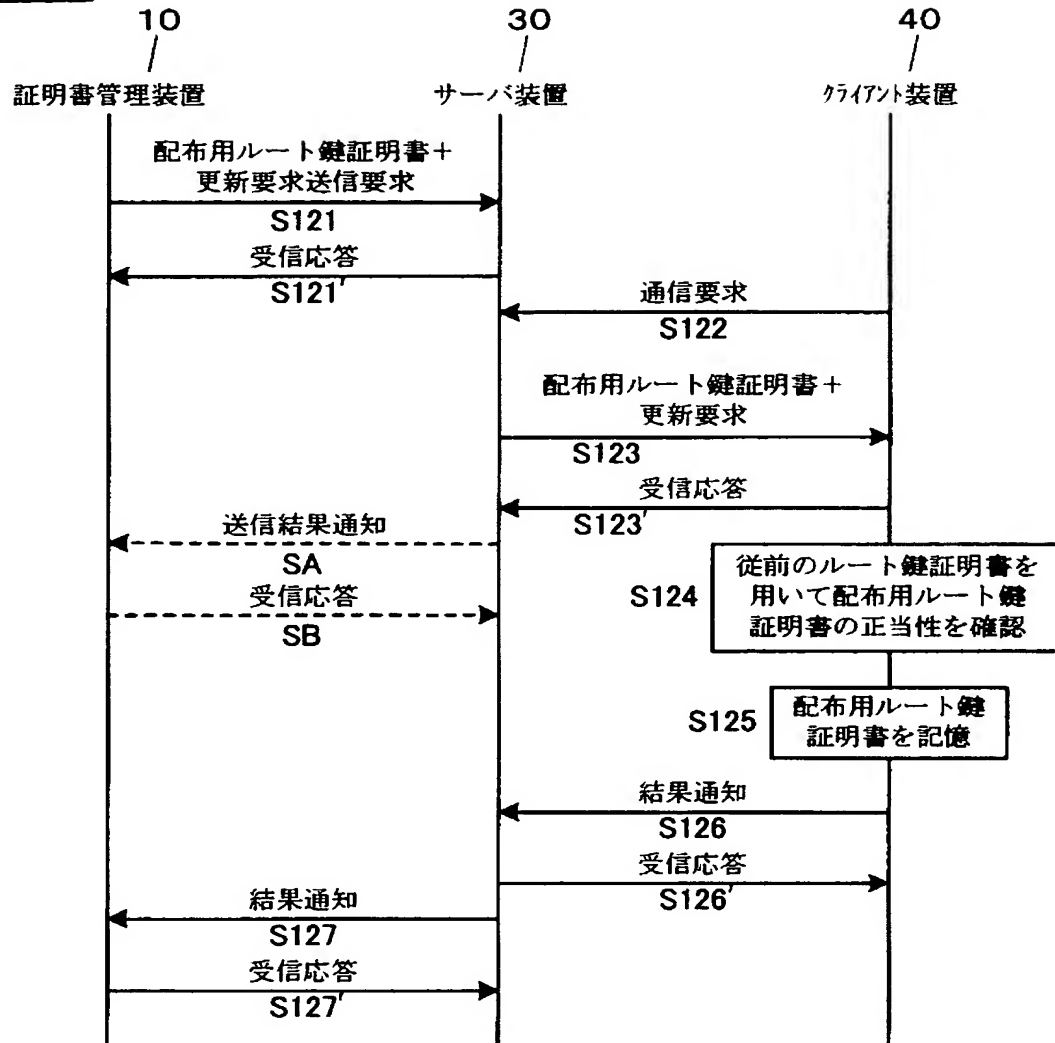


【図 14】

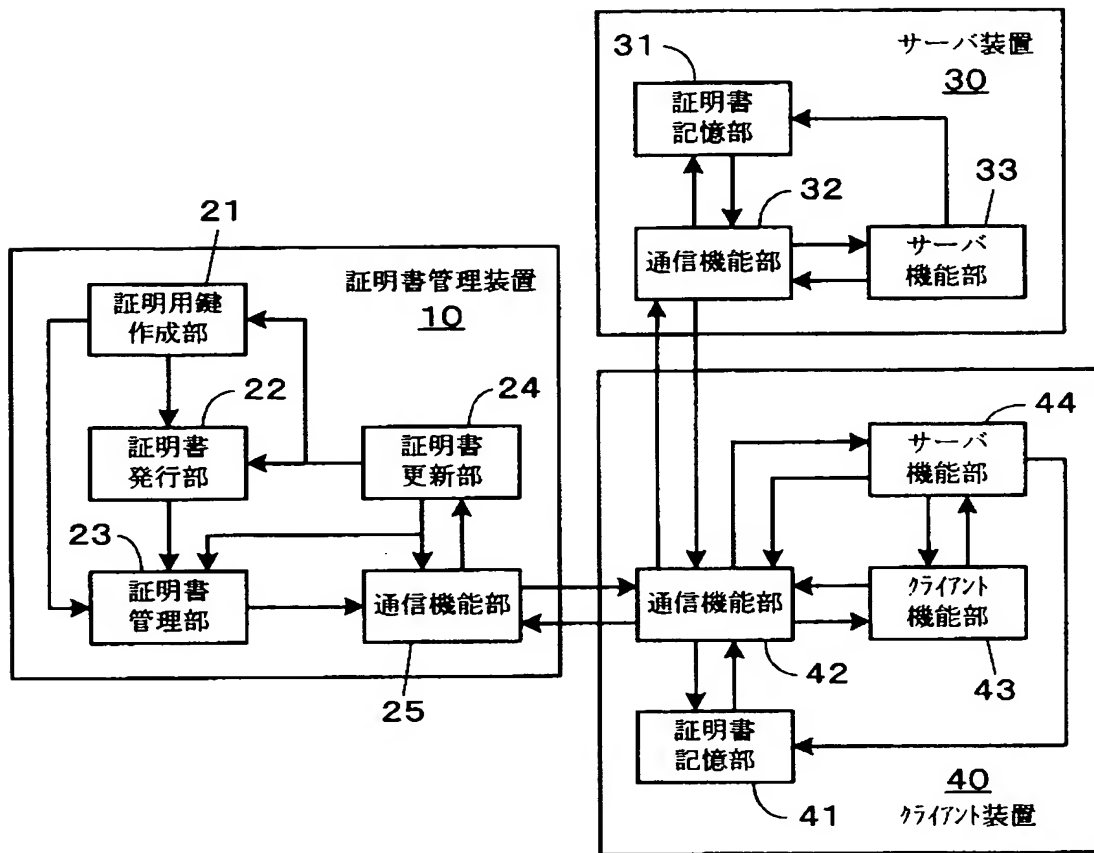
処理1'

【図15】

## 処理2'

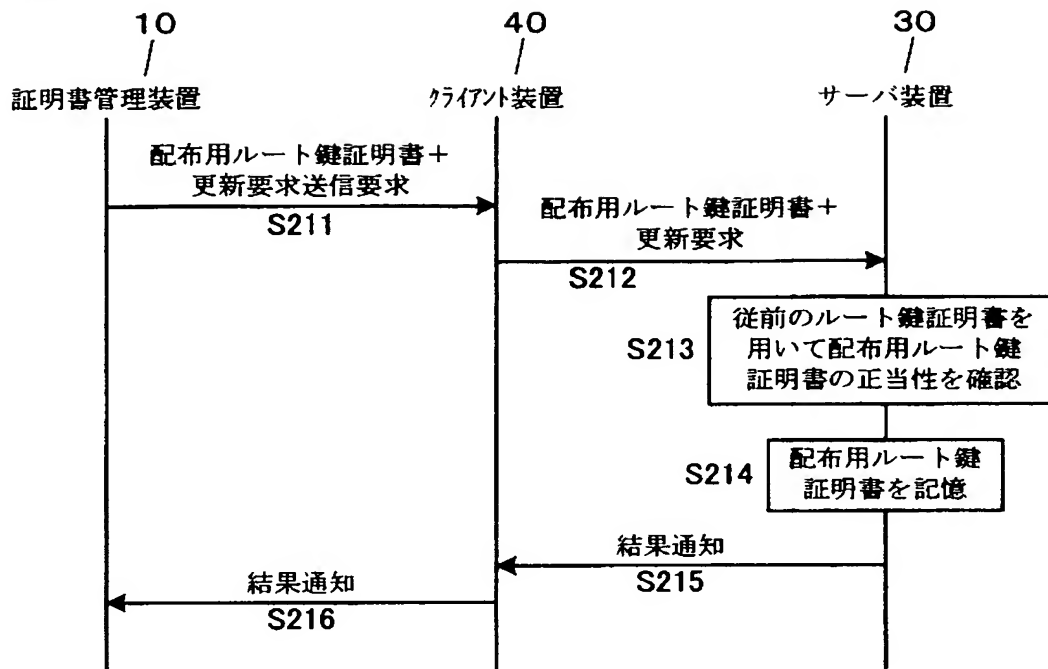


【図 16】



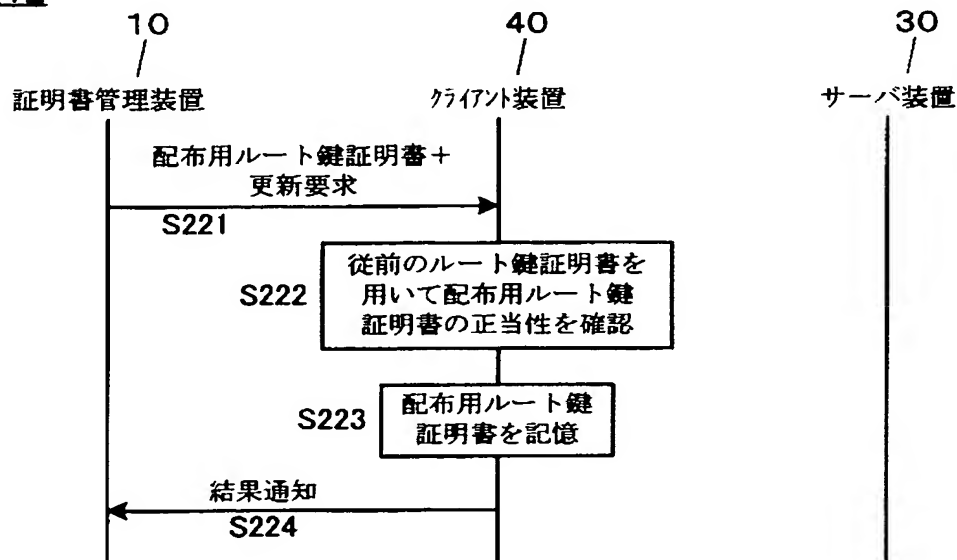
【図 17】

## 処理11

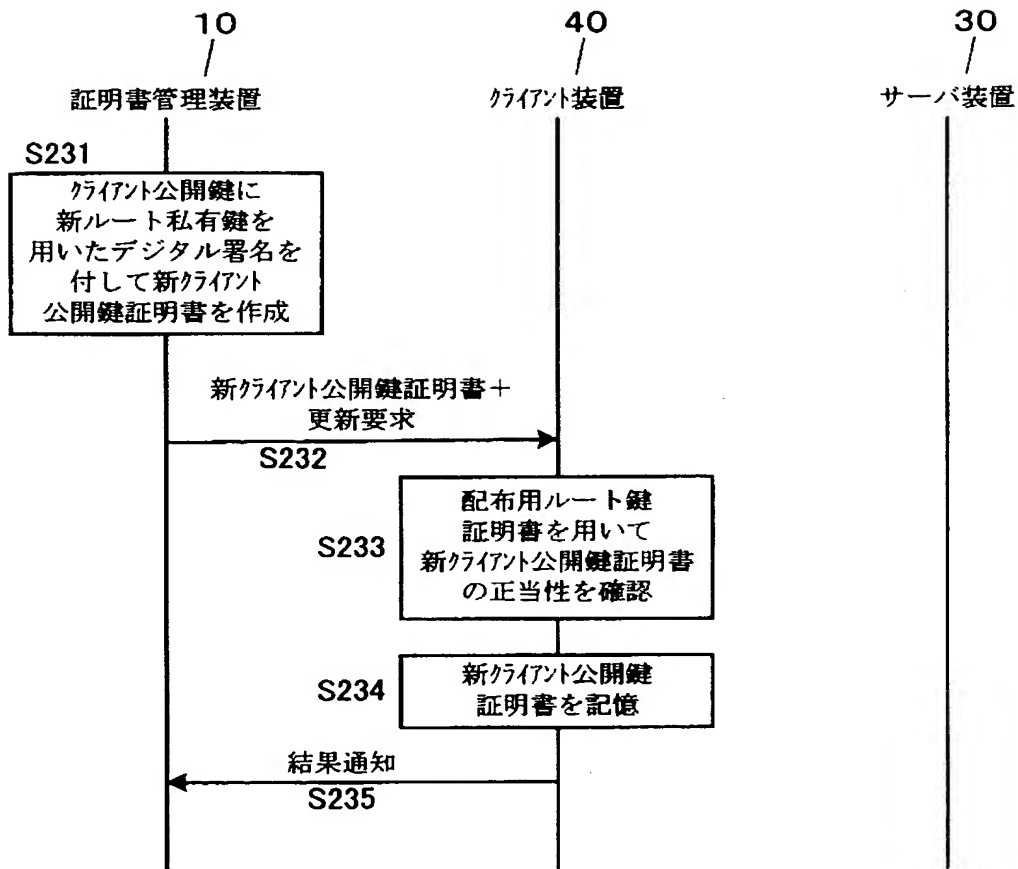


【図 18】

## 処理12

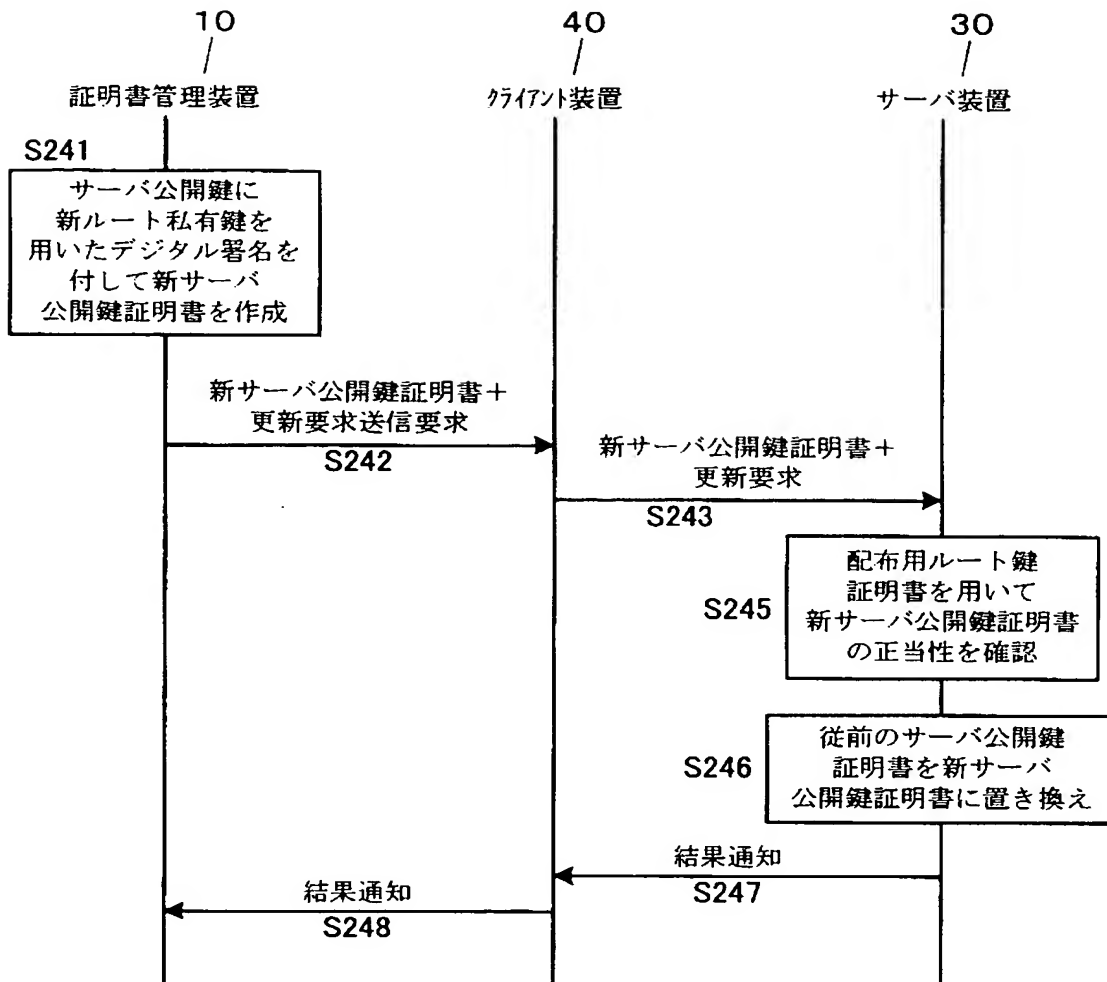


【図 19】

処理13

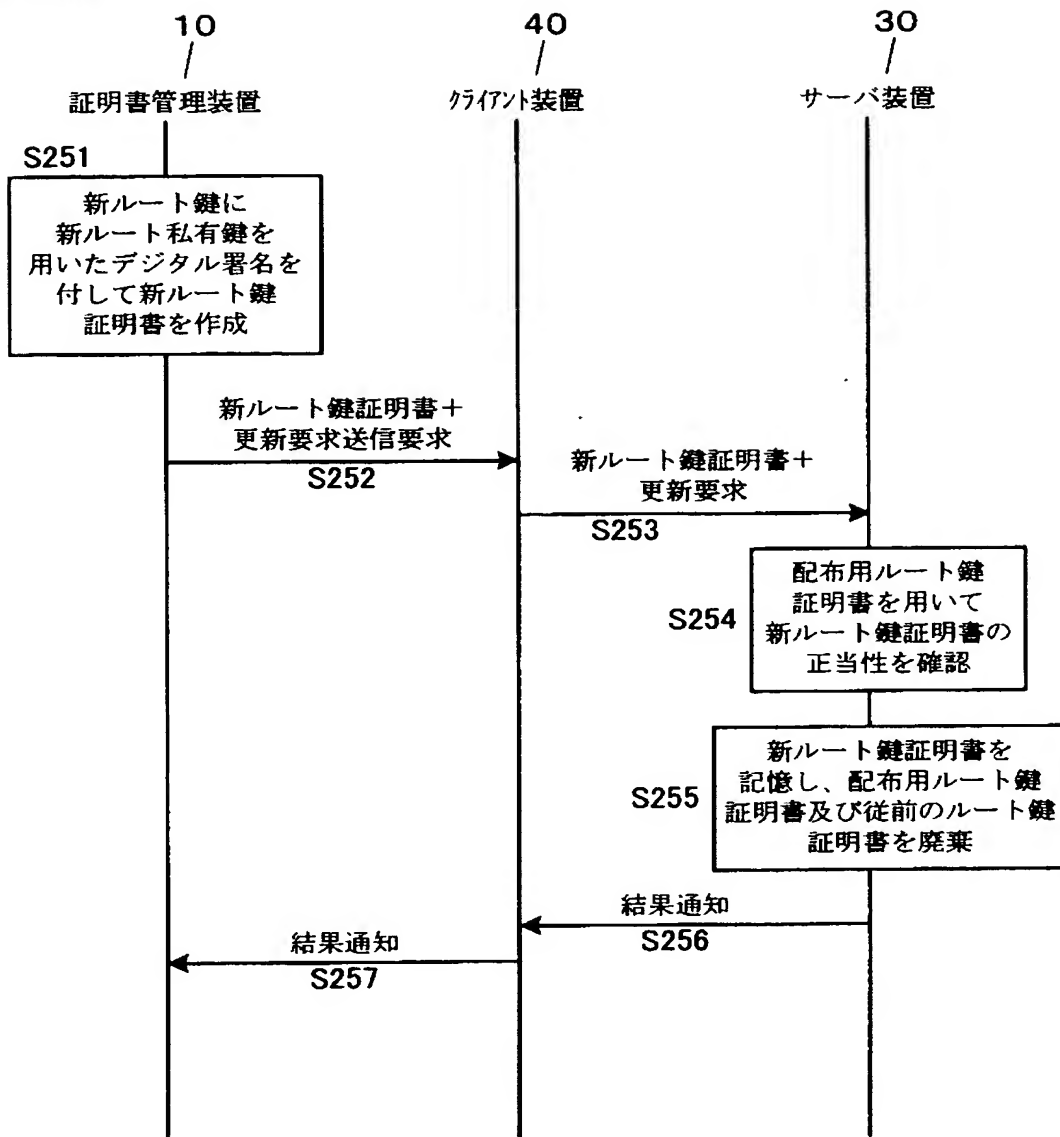
【図 20】

## 処理14



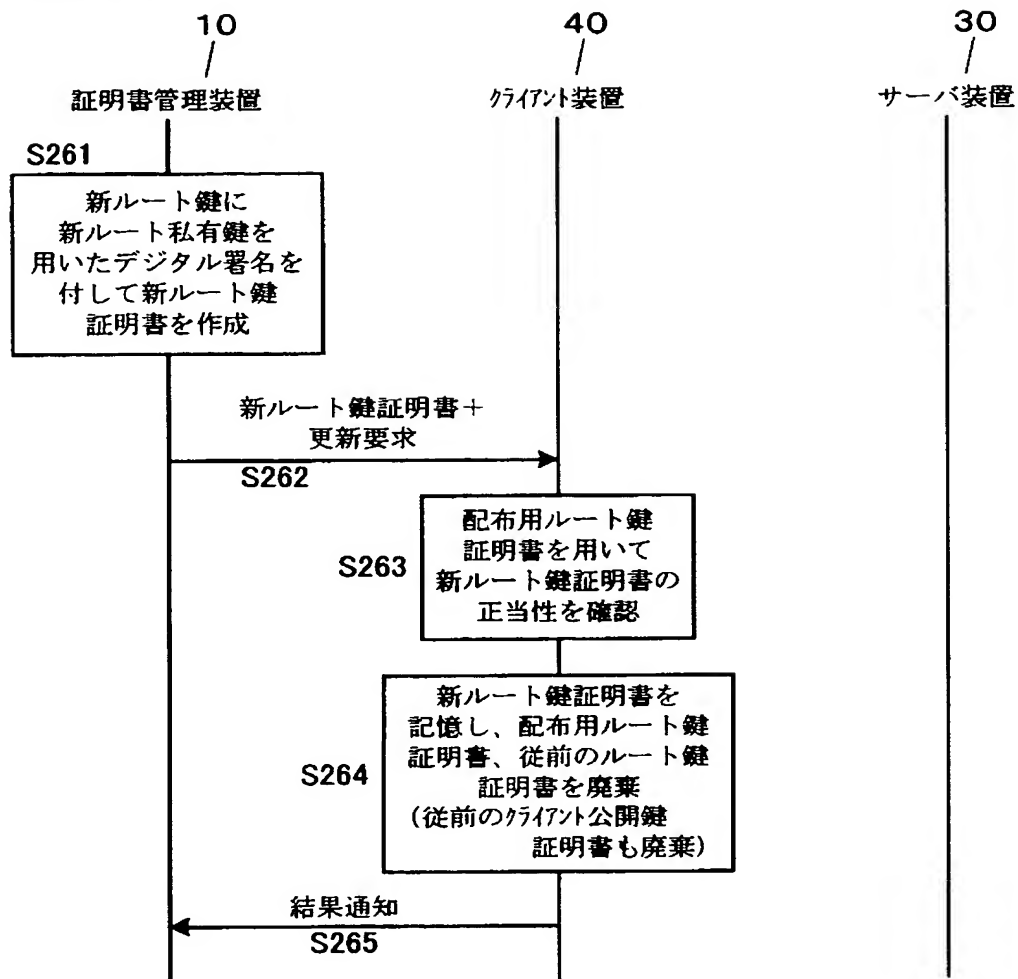
【図 21】

## 処理15

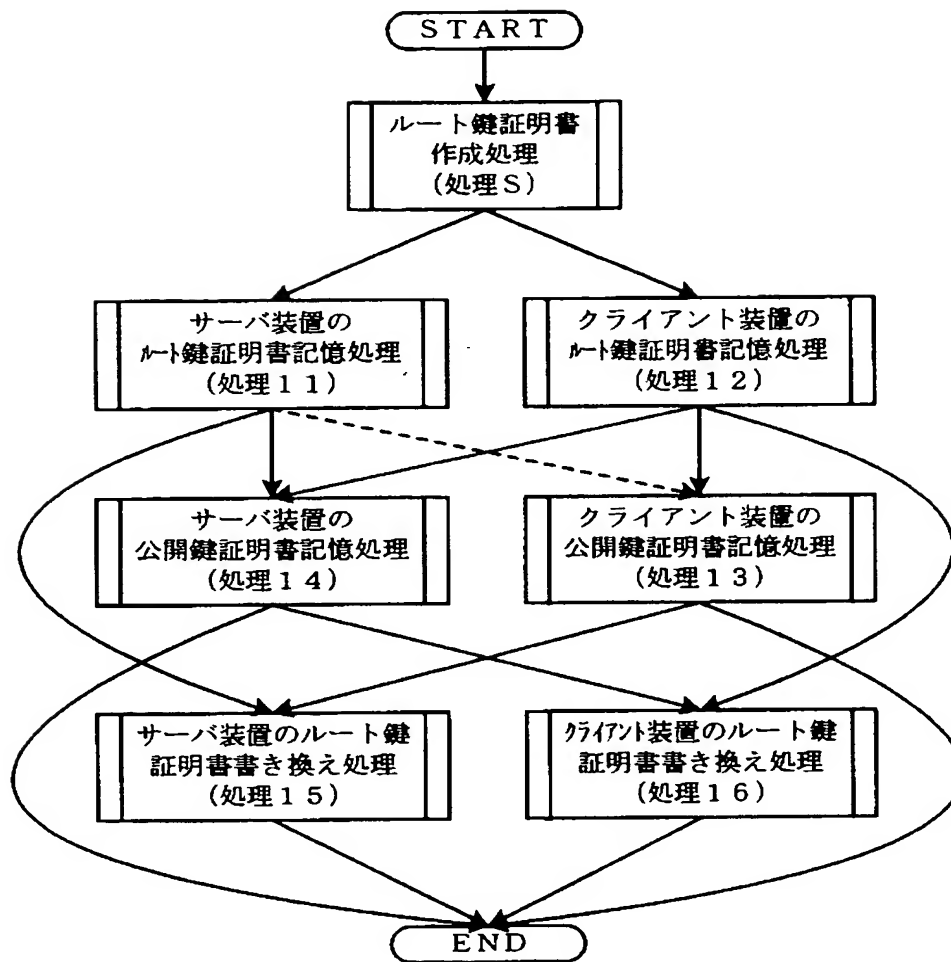




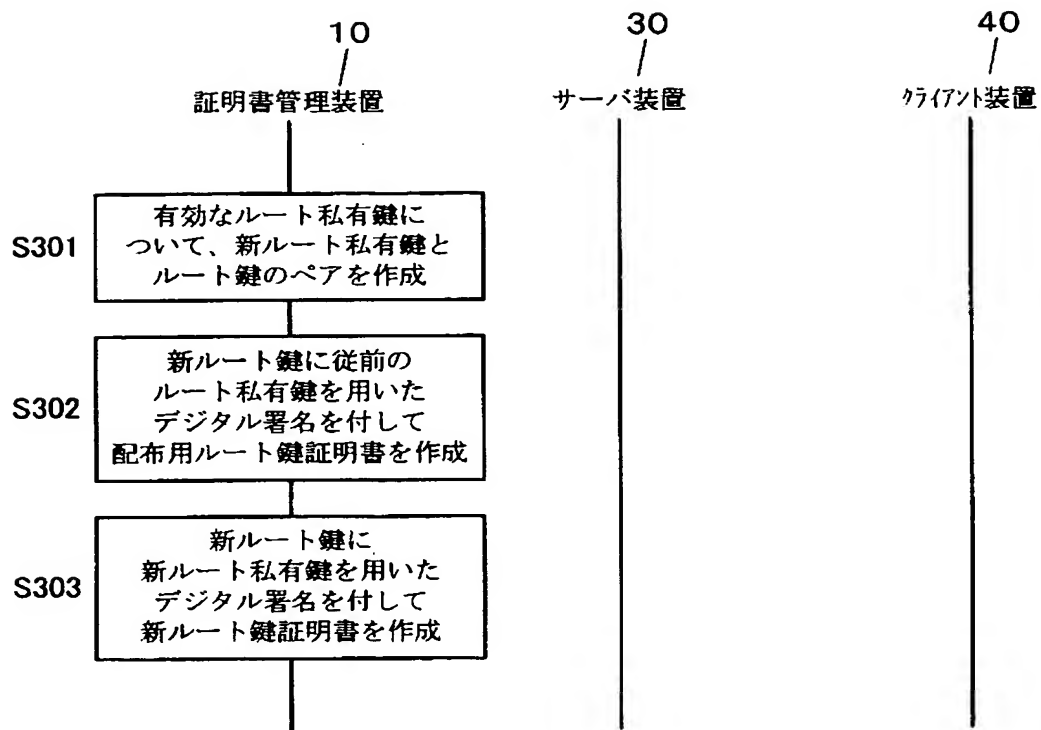
【図 22】

処理16

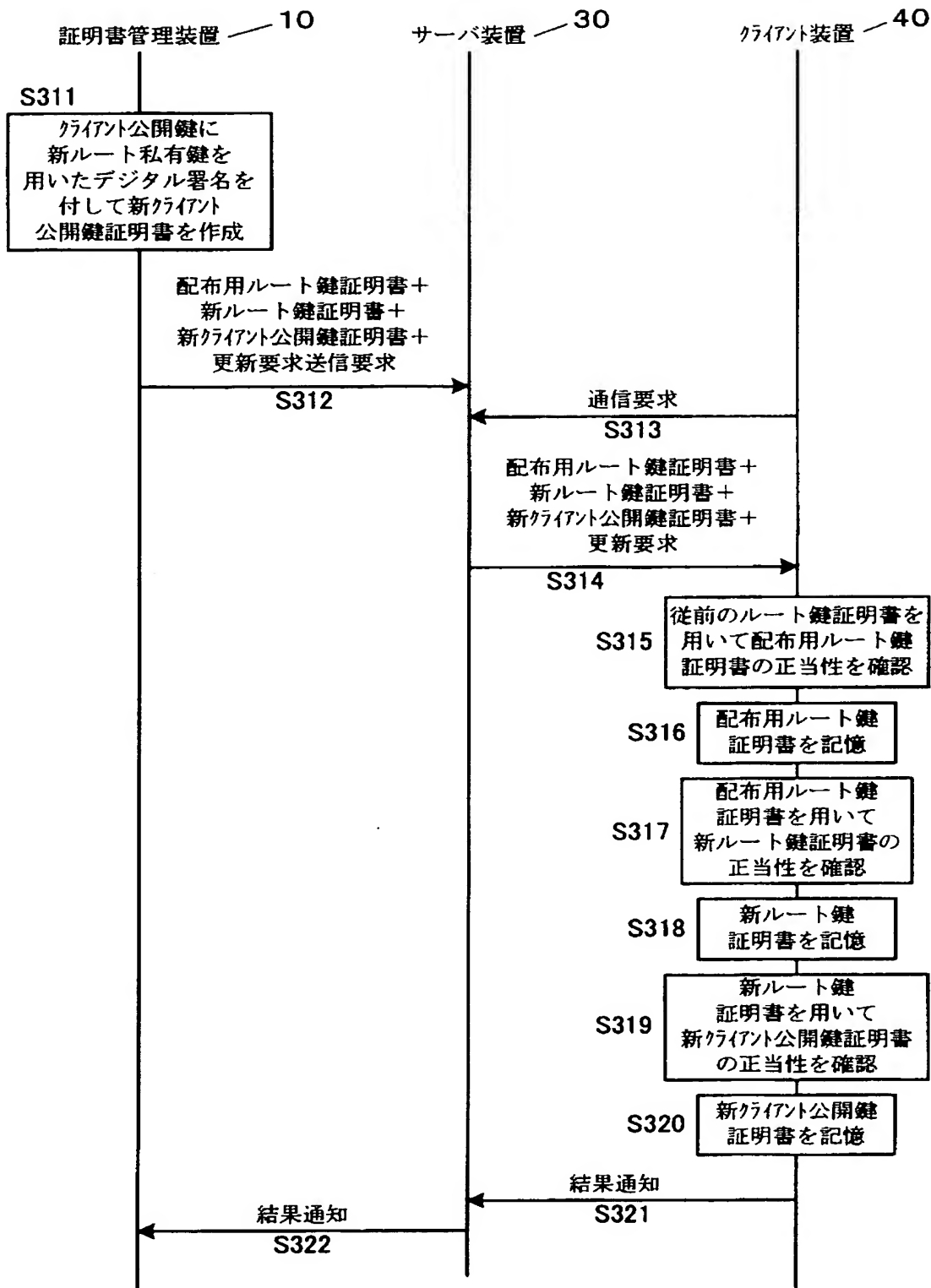
【図 23】



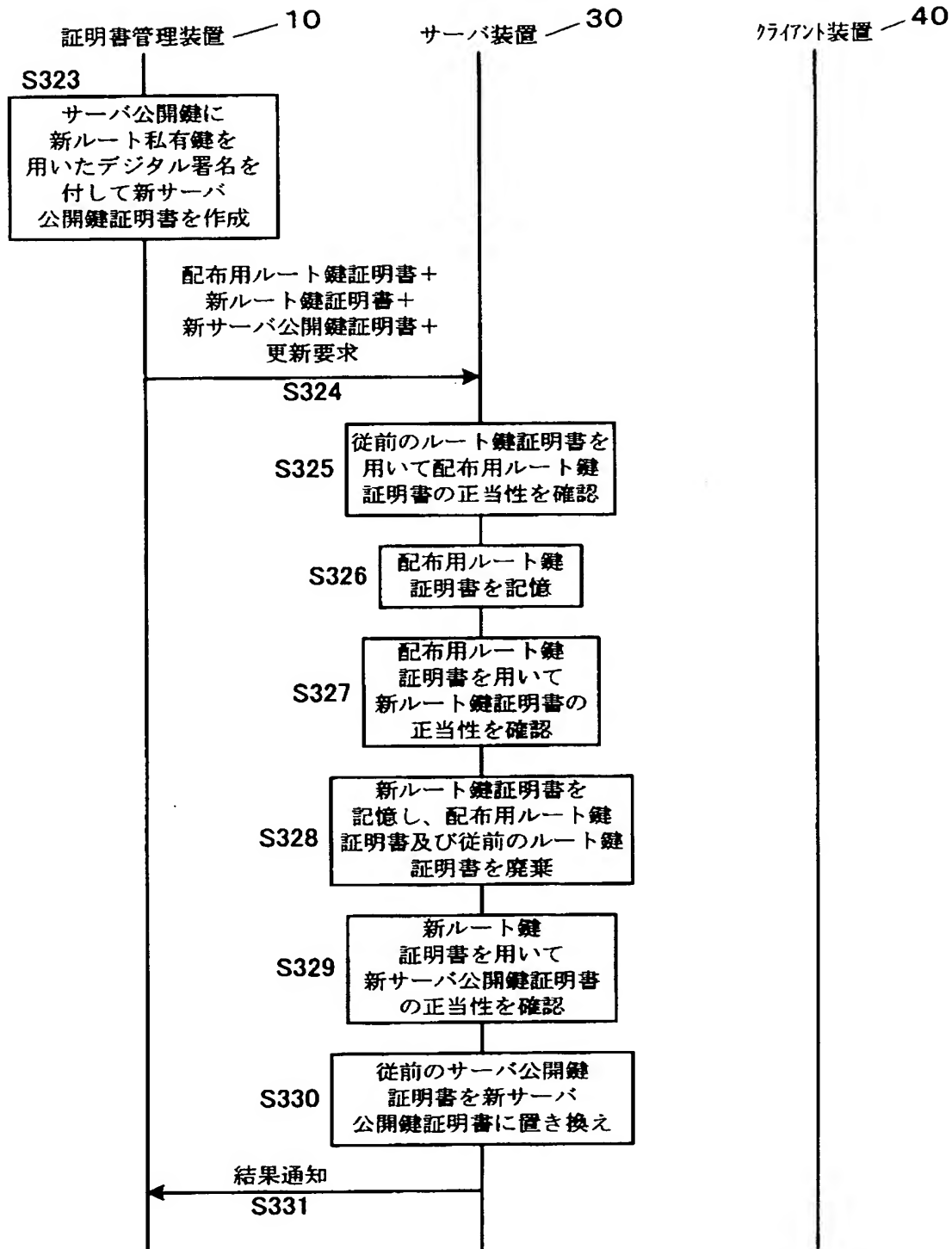
【図 24】



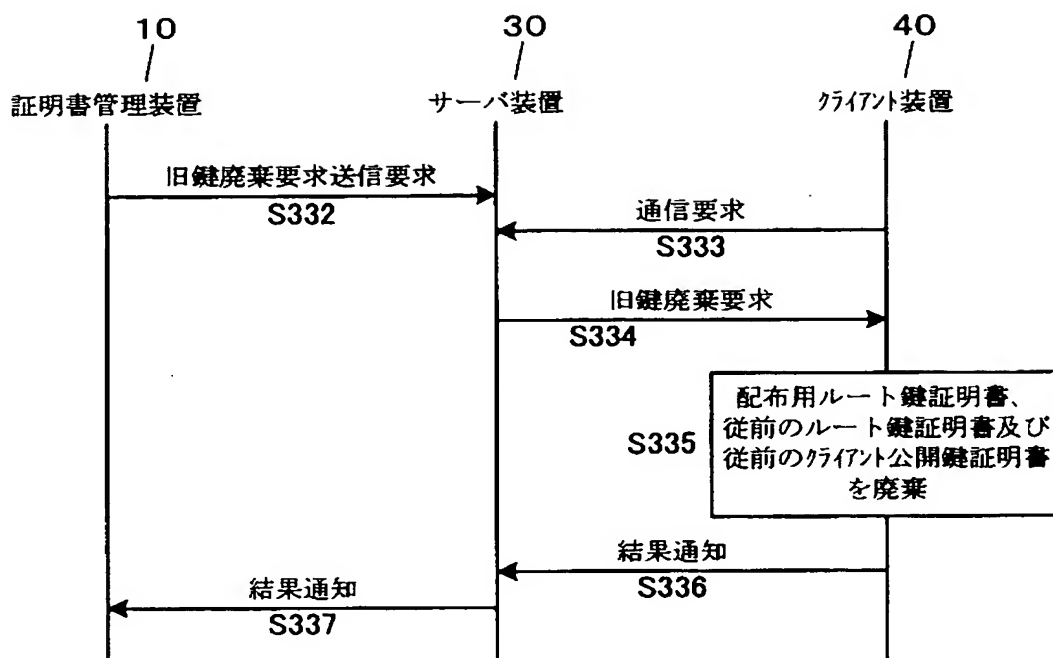
【図 25】



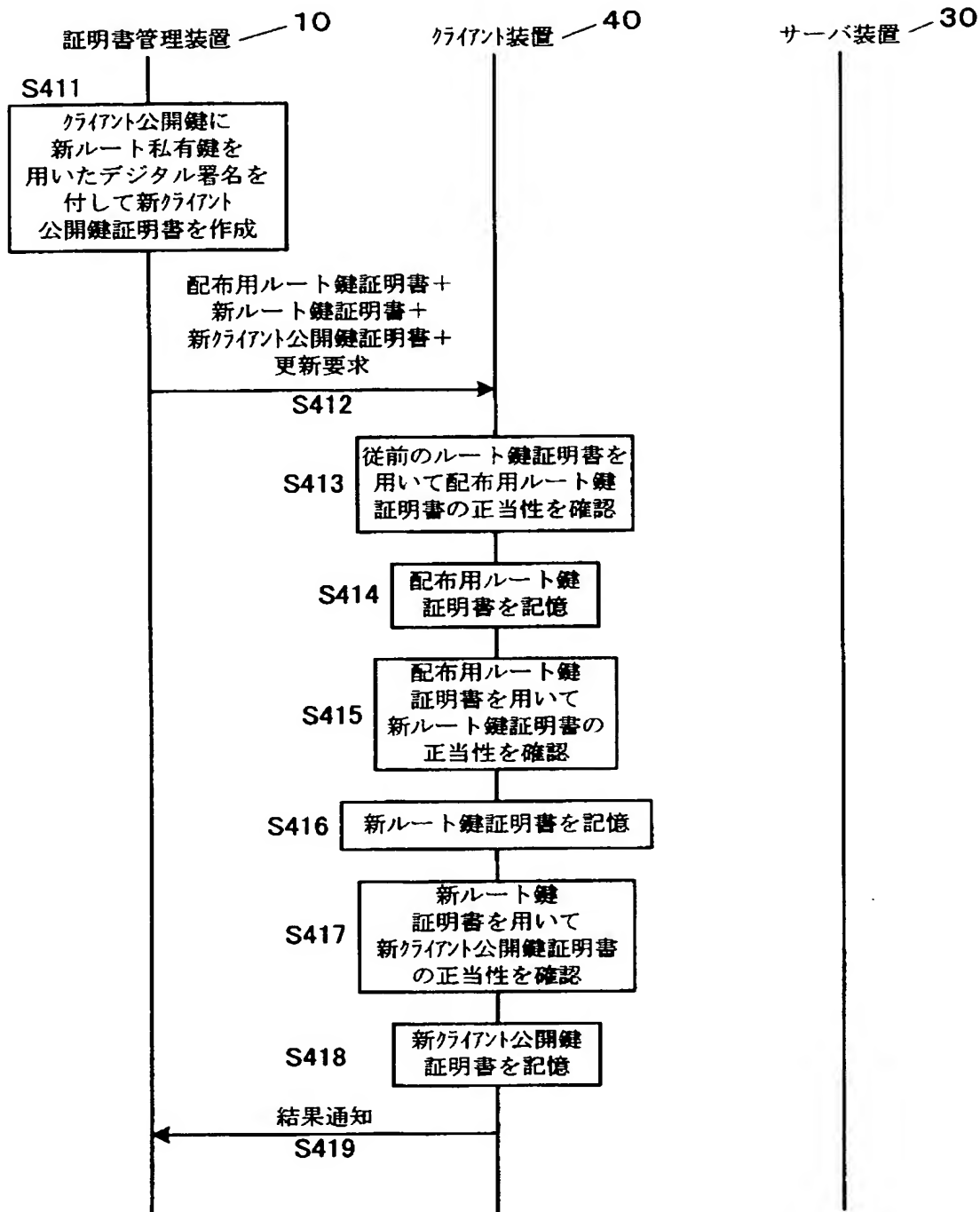
【図 26】



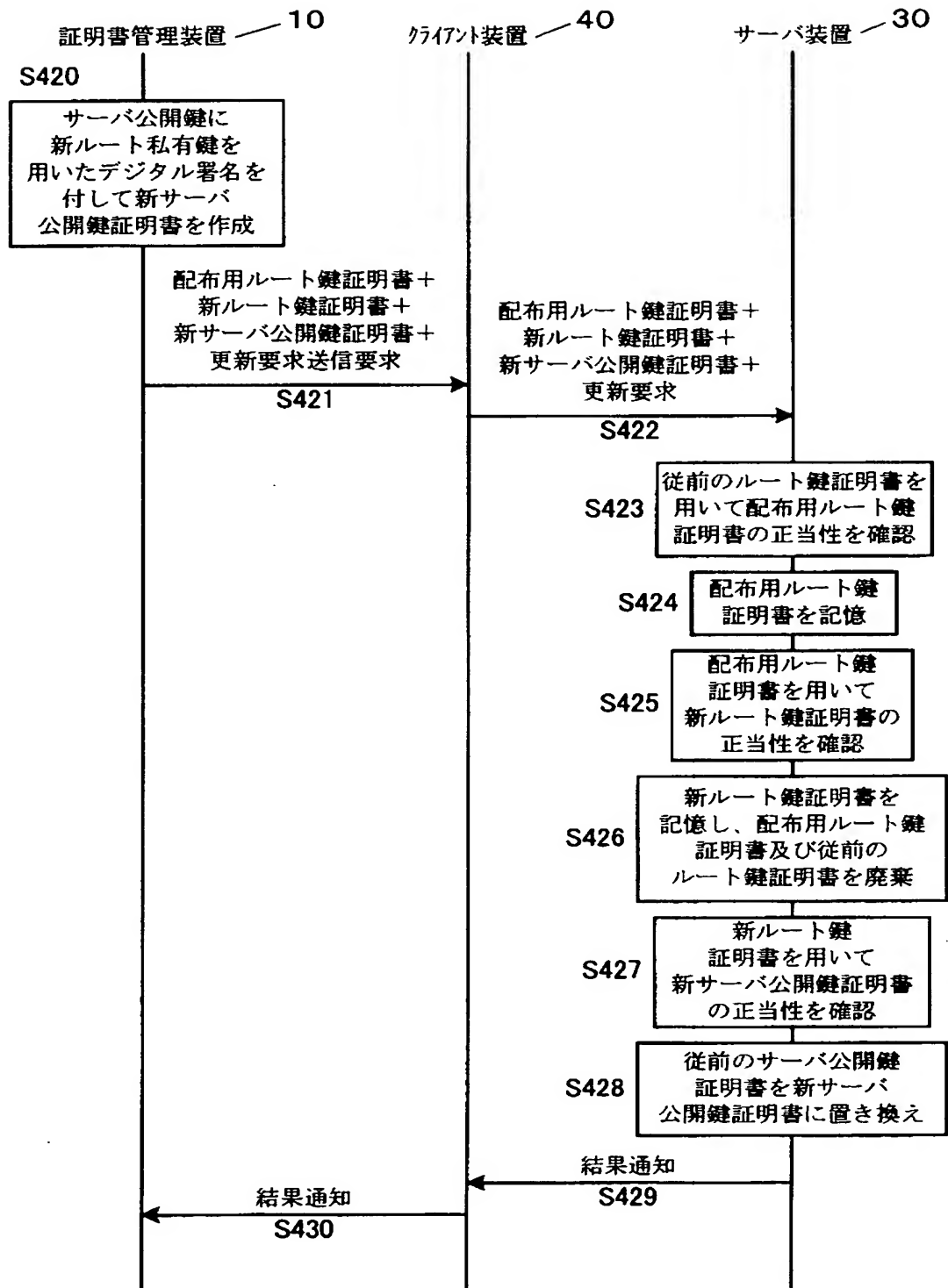
【図 27】



【図 28】

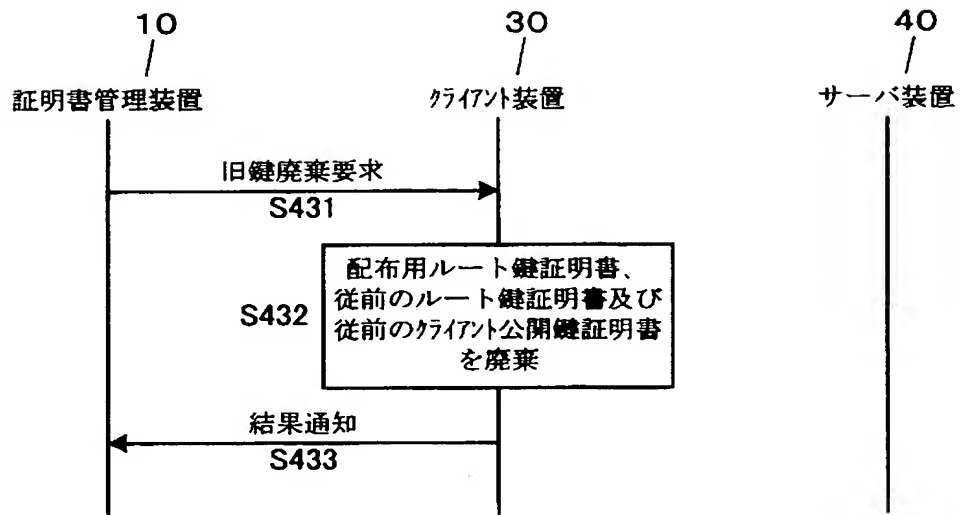


【図 29】

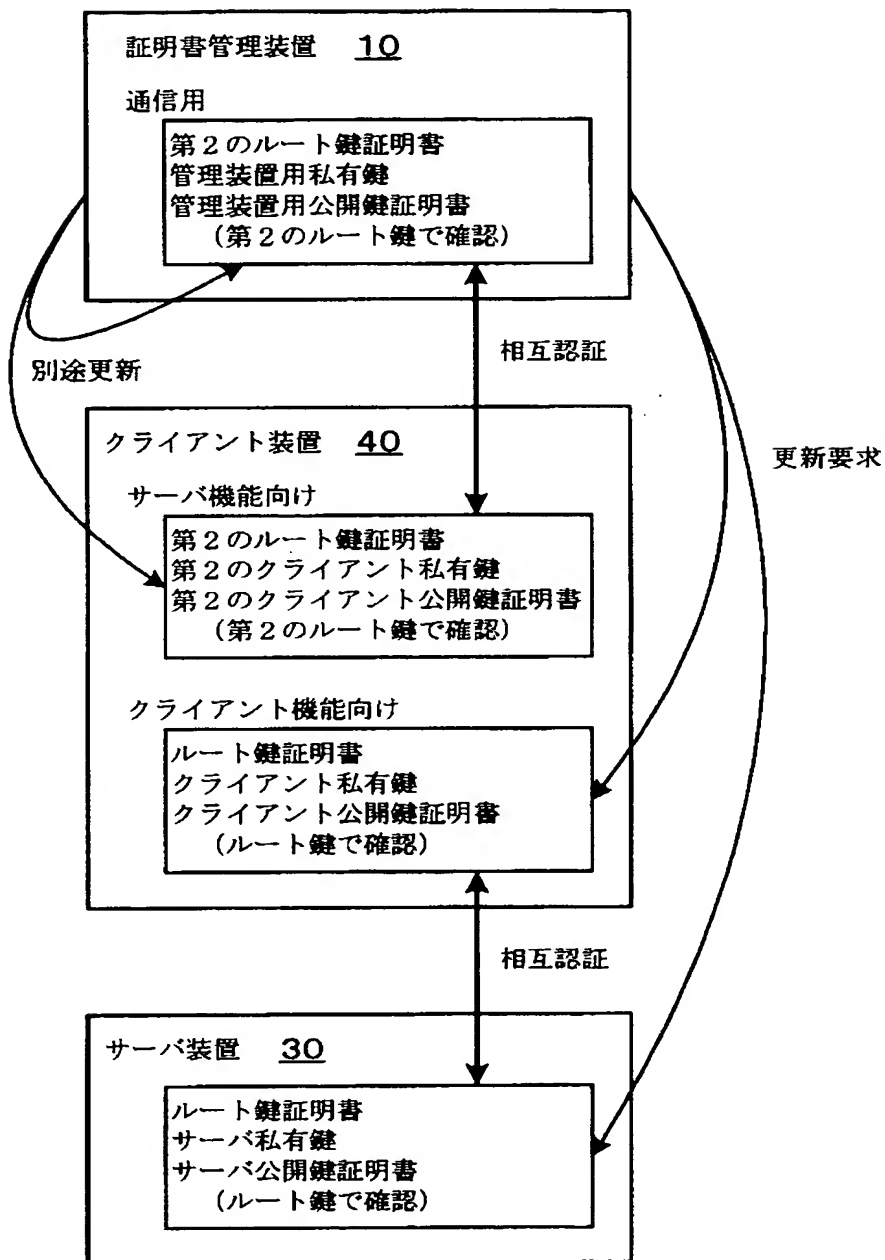




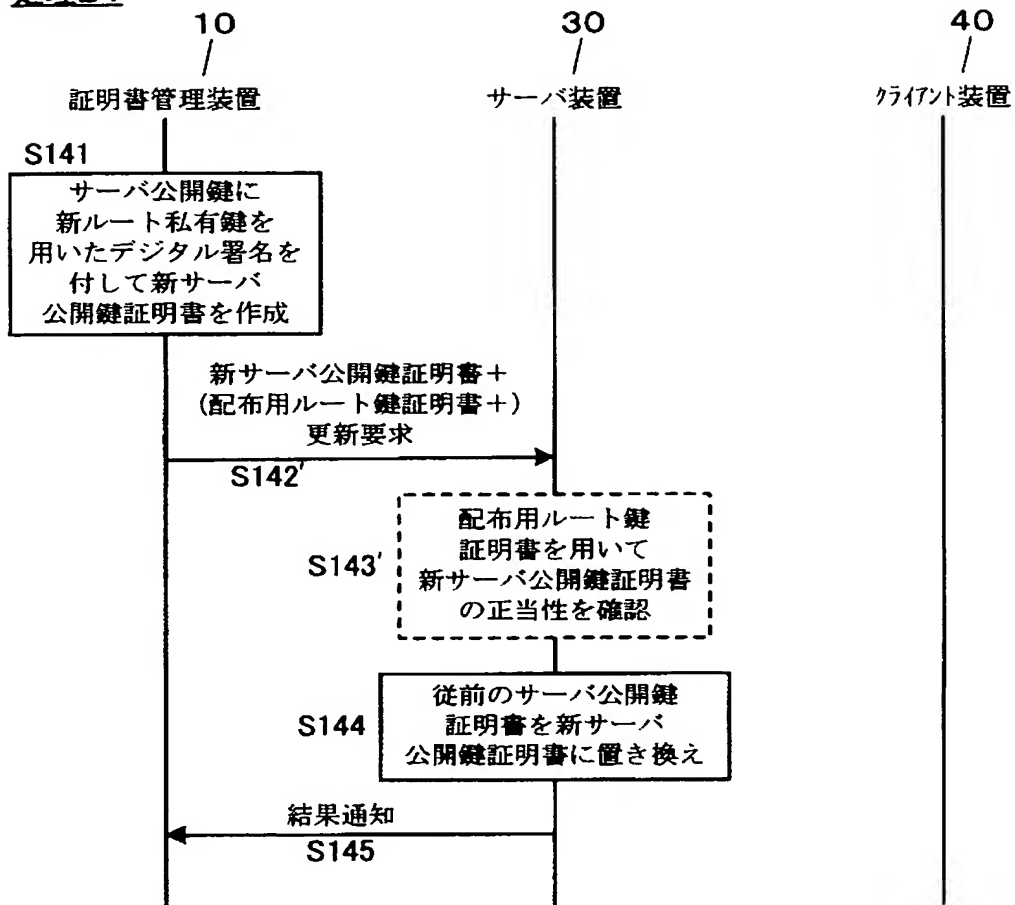
【図 30】



【図 31】

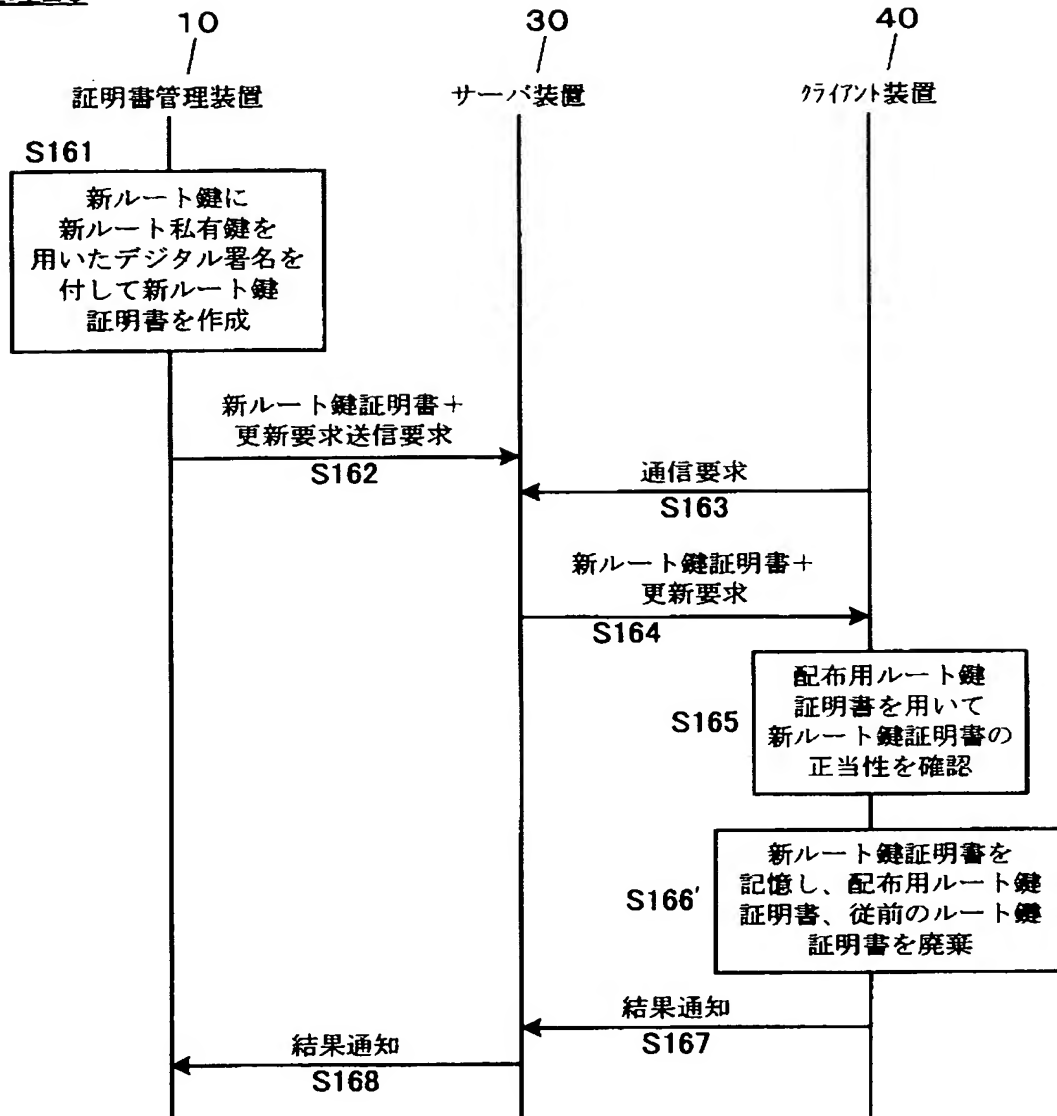


【図 32】

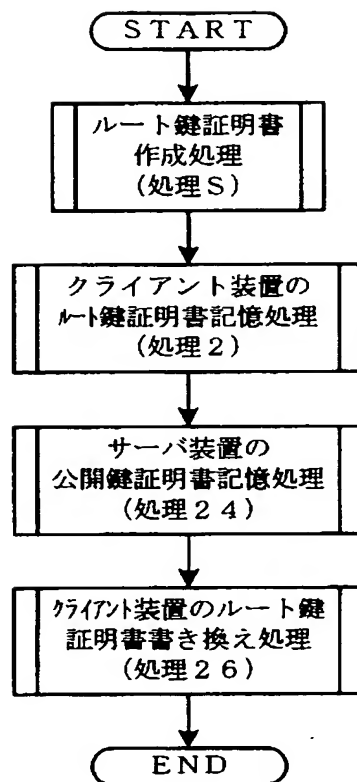
処理24

【図 33】

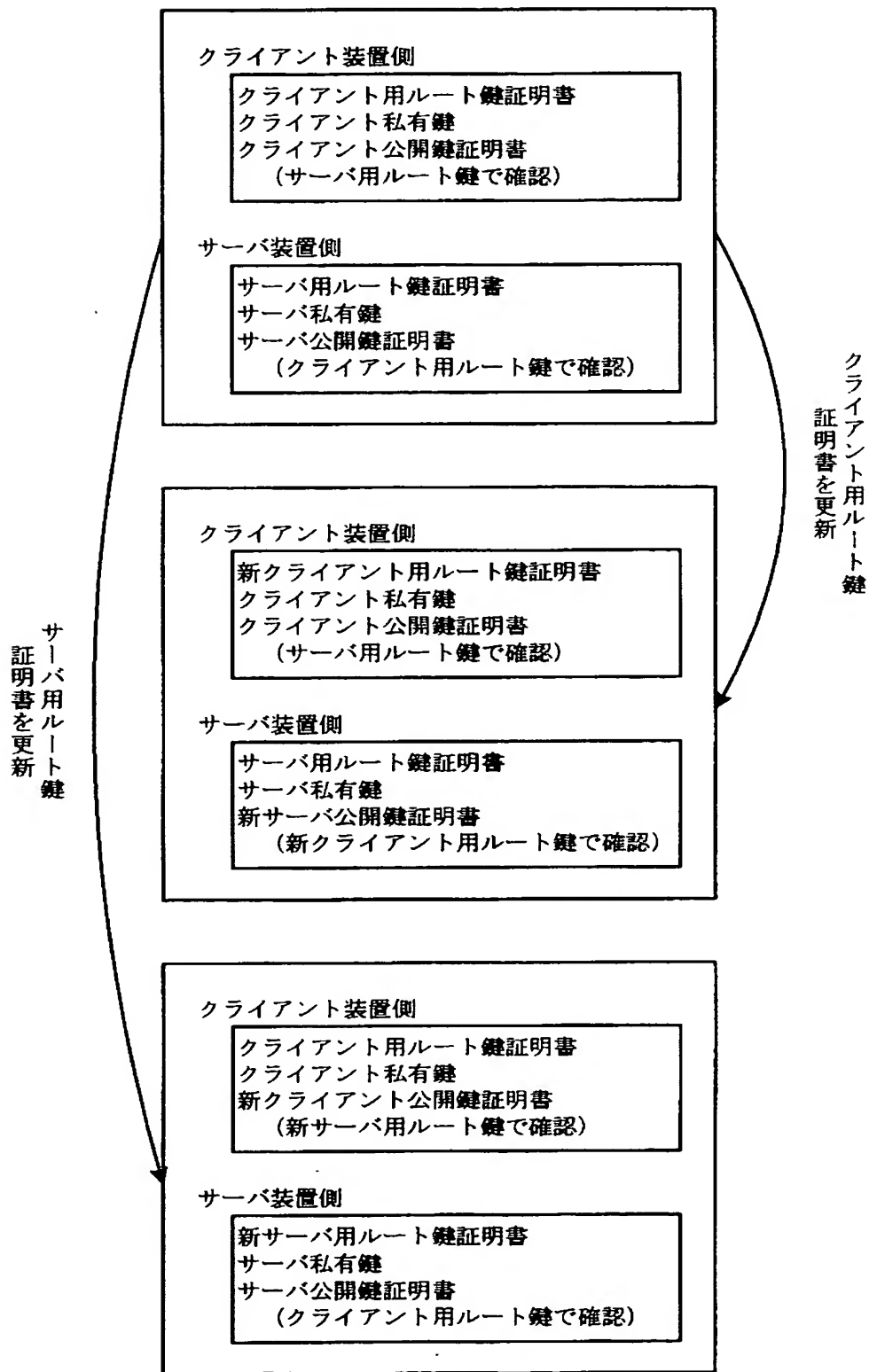
## 処理26



【図 34】

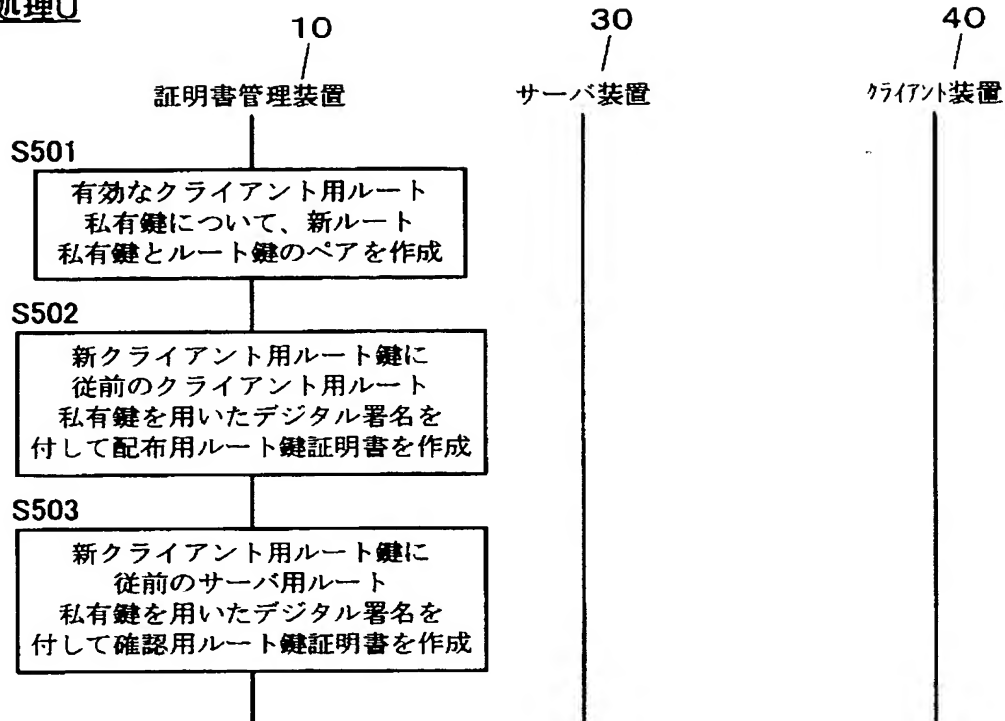


【図 35】



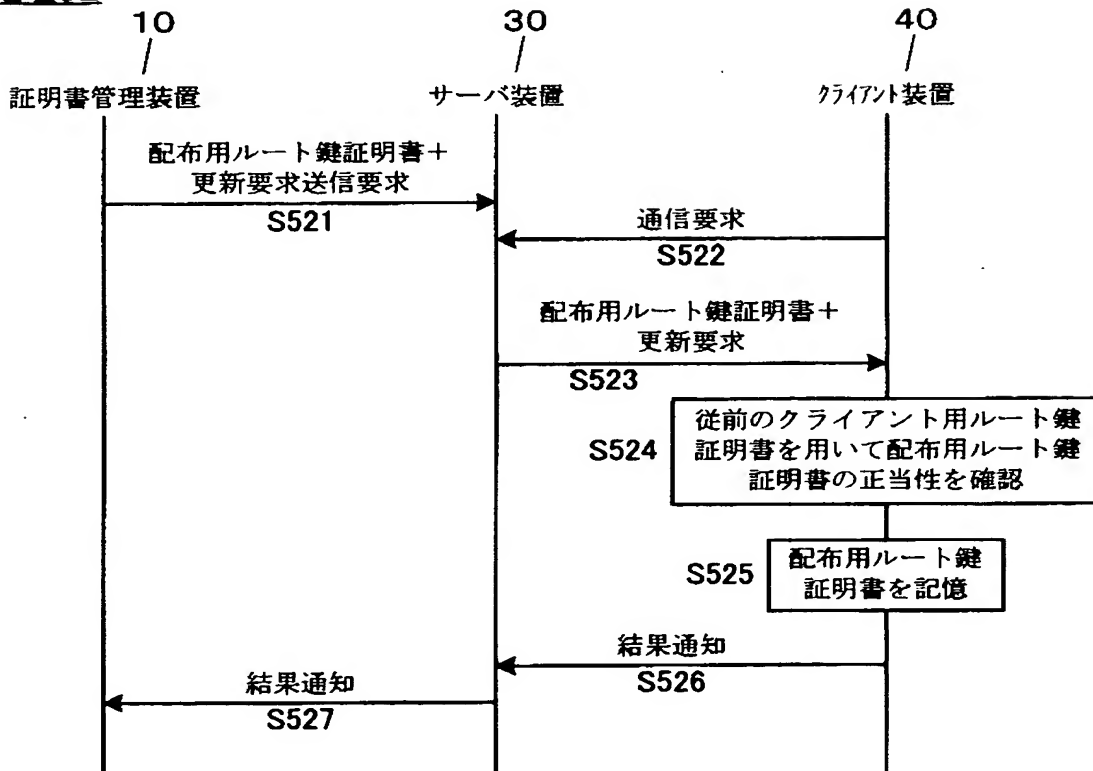
【図 36】

## 処理U



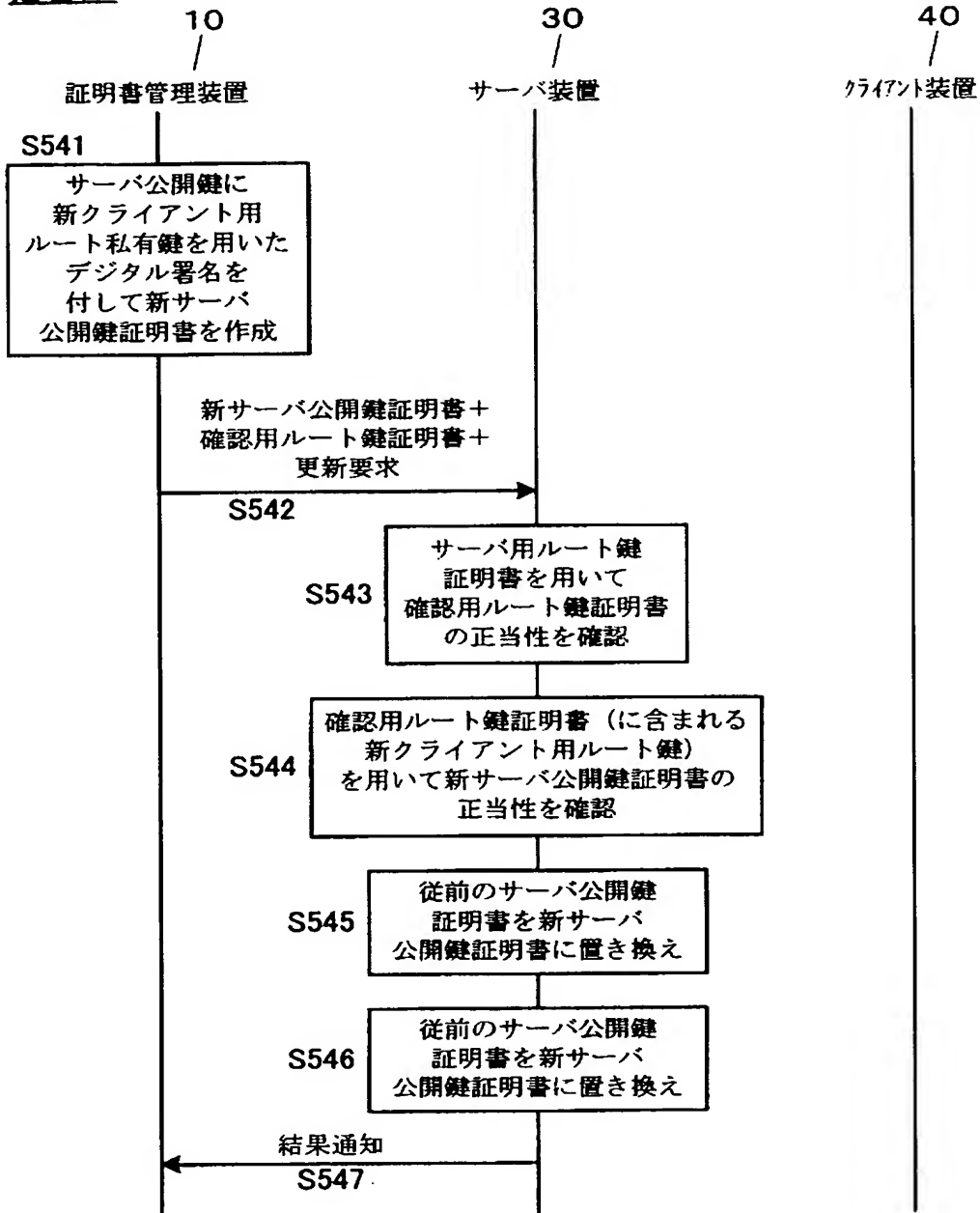
【図 37】

## 処理32



【図 38】

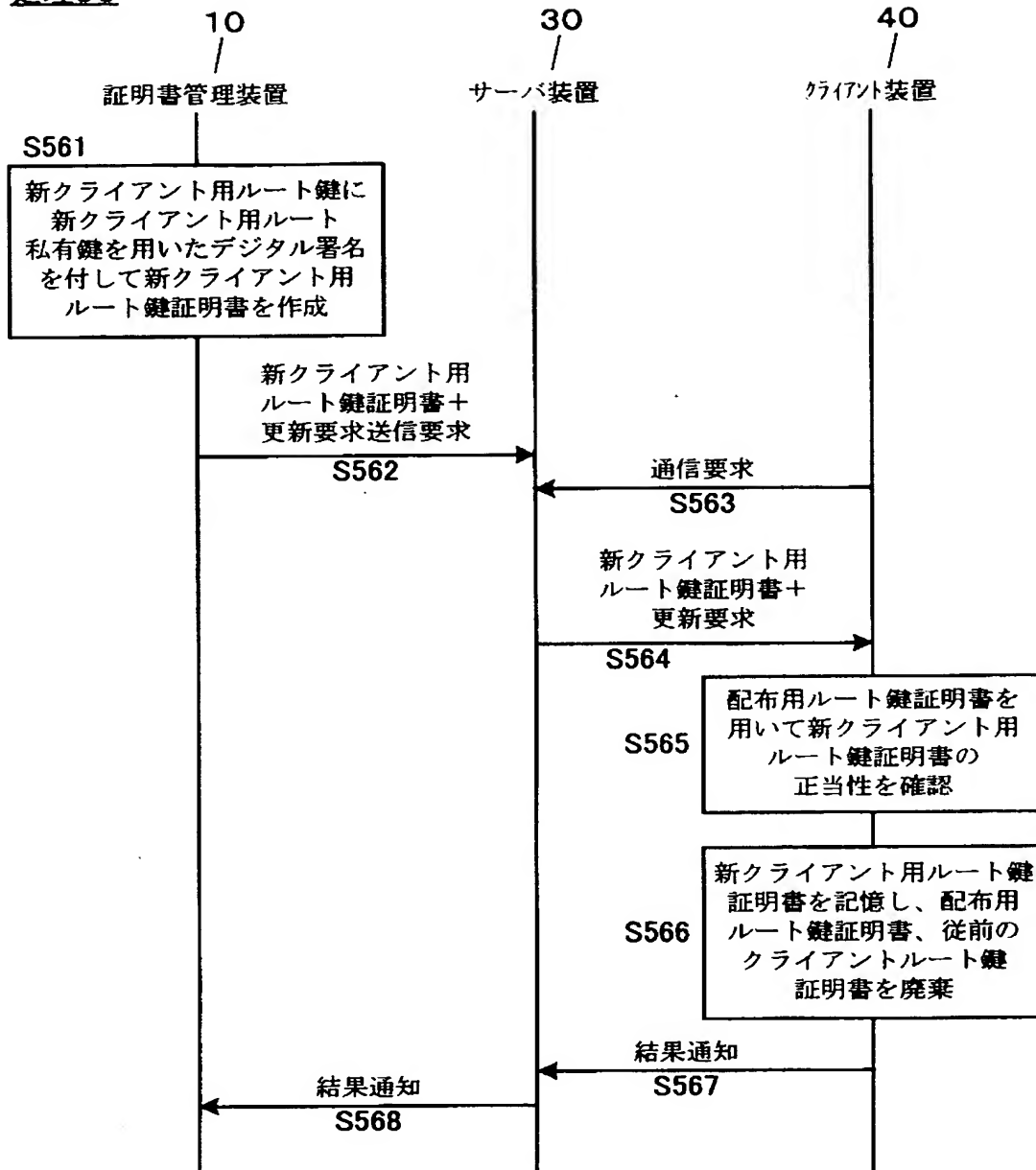
## 処理34



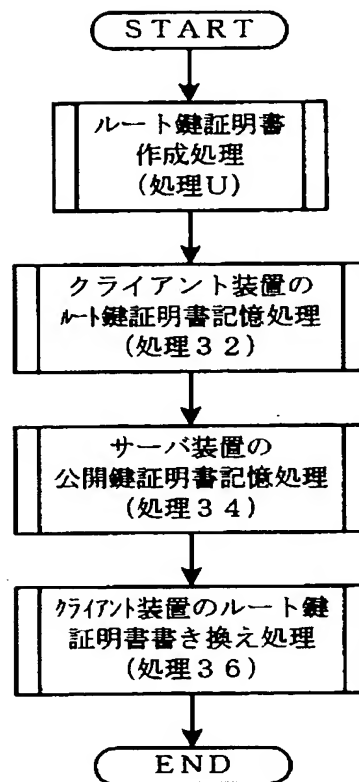


【図 39】

## 処理36

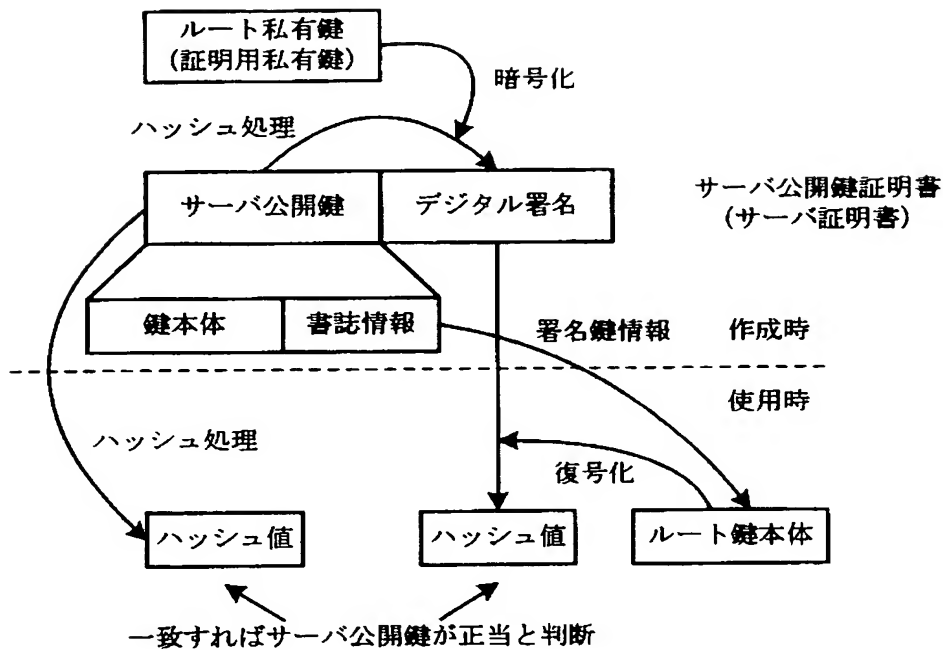


【図 40】

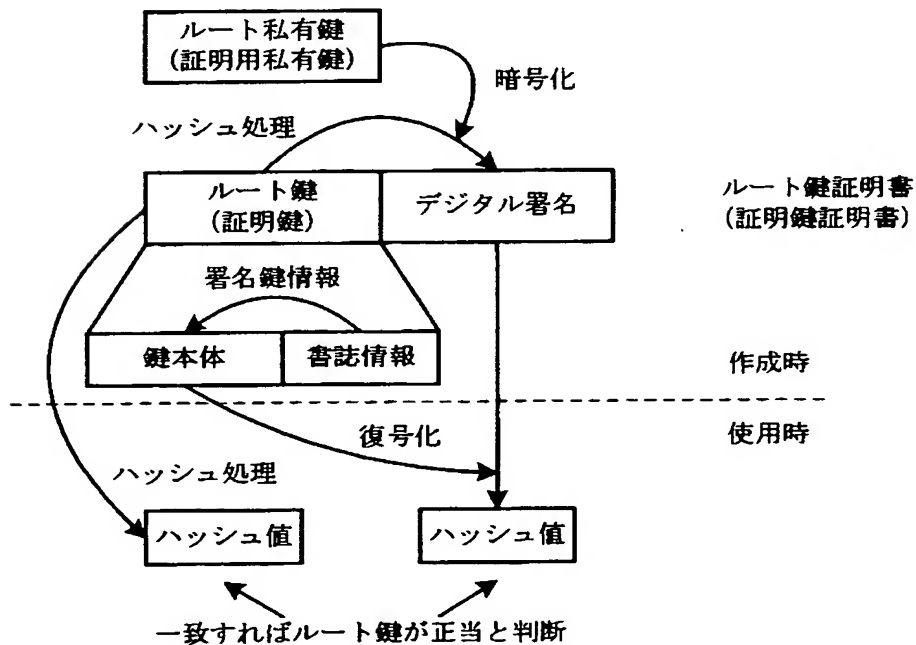


【図 41】

(a)



(b)



【書類名】 要約書

【要約】

【課題】 クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性確認に用いるルート鍵を自動的に更新できるようにする。

【解決手段】 クライアント装置とサーバ装置との間で通信を確立する際に公開鍵暗号を利用したデジタル証明書を用いるSSL等の方式による認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムに、デジタル証明書管理装置を接続し、サーバ装置とクライアント装置のルート鍵を自動的に更新するデジタル証明書管理システムを構成する。そして、この更新処理において、サーバ装置に公開鍵証明書を送信する処理（処理4）を、クライアント装置に新ルート鍵を送信する処理（処理2）の後で行うようにする。

【選択図】 図13

特願 2 0 0 4 - 0 5 6 7 6 4

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 6 7 4 7 ]

1. 変更年月日 2 0 0 2 年 5 月 1 7 日

[変更理由] 住所変更

住 所 東京都大田区中馬込 1 丁目 3 番 6 号

氏 名 株式会社リコー